Dr.WEB®

Enterprise Security Suite

Defend what you create

# Manuale dell'amministratore

**© 2004-2013 Doctor Web. Tutti i diritti riservati**

Materiali, riportati in questo documento, sono di proprietà di Doctor Web e si possono utilizzare esclusivamente per uso personale dell'acquirente del prodotto. Nessuna parte di tale può essere copiata, riprodotta su una risorsa di rete o trasmessa per canali di comunicazione o via mass media o utilizzata in altro modo oltre uso personale, se non facendo riferimento alla fonte.

MARCHI
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk e il logotipo Dr.WEB sono marchi commerciali registrati di Doctor Web in Russia e/o in altri paesi. Altri marchi commerciali registrati, logotipi o denominazioni delle società, nominati nel presente documento, sono di proprietà dei loro titolari.

LIMITAZIONE DI RESPONSABILITÀ
Doctor Web e i suoi fornitori sono in ogni caso esenti di qualsiasi responsabilità per errori e/o omissioni, presenti nel presente documento, e per danni (diretti o indiretti, incluso un profitto perso) causati da essi all'acquirente del prodotto.

**Dr.Web Enterprise Security Suite**
**Versione 6.0.4**
**Manuale dell'amministratore**
**10.07.2013**

Doctor Web, Sede centrale in Russia
125124
Russia, Mosca,
via 3 Yamskogo Polya, tenuta 2, edificio 12A

Sito web: www.drweb.com
Telefono: +7 (495) 789-45-87

Le informazioni sulle sedi rappresentative si trovano sul sito ufficiale dell'azienda.

# Doctor Web

Doctor Web è uno sviluppatore russo di sistemi di sicurezza informatica.

Doctor Web offre valide soluzioni di protezione antivirus e antispam per enti pubblici, aziende e utenti privati.

I programmi antivirali della famiglia Dr.Web vengono sviluppati a partire dal 1992, sempre raggiungono i migliori risultati nel rilevamento di malware e corrispondono agli standard internazionali di sicurezza.

I certificati e premi conferiti ai prodotti Dr.Web provano il loro avanzato grado di affidabilità. Gli utenti di Dr.Web si trovano in diverse parti del mondo.

**Ringraziamo i nostri utenti per la fiducia che hanno nelle soluzioni della famiglia Dr.Web!**

# Sommario

**Capitolo 1. Introduzione** 13

**1.1. Introduzione** 13

**1.2. Segni convenzionali e abbreviazioni** 15

**1.3. Contenuti, destinazione e funzionalità principali di Dr.Web Anti-virus Enterprise Security Suite** 16

**1.4. Vantaggi** 20

**1.5. Requisiti di sistema** 21

**1.6. Set di fornitura** 28

**1.7. File chiavi** 29

**Capitolo 2. Installazione e eliminazione dei componenti di Dr.Web Enterprise Security Suite** 32

**2.1. Creazione rete antivirus** 32

**2.2. Installazione diDr.Web Enterprise Server** 33

2.2.1. Installazione di Dr.Web Enterprise Server per i SO Windows® 34

2.2.2. Installazione di Dr.Web Enterprise Server per i SO della famiglia UNIX® 46

2.2.3. Installazione del plugin Dr.Web Browser-Plugin 52

**2.3. Installazione di Dr.Web Enterprise Agent per SO Windows®** 55

2.3.1. File di installazione 56

2.3.2. Installazione di Dr.Web Enterprise Agent con il pacchetto di installazione 58

2.3.3. Installazione di Dr.Web Enterprise Agent con Installazione di rete 64

**2.4. Installazione remota di Dr.Web Enterprise Agent per i SO Windows® 70**

2.4.1. Installazione di Dr.Web Enterprise Agent con il Centro gestione di Dr.Web **73**

2.4.2. Installazione di Dr.Web Enterprise Agent con il servizio Active Directory **80**

**2.5. Installazione di NAP Validator 87**

**2.6. Installazione di Server proxy 88**

**2.7. Eliminazione dei componenti singoli di Dr.Web Enterprise Security Suite 92**

2.7.1. Eliminazione dei componenti del software per i SO Windows® **92**

2.7.2. Eliminazione di Dr.Web Enterprise Agent con il servizio Active Directory **95**

2.7.3. Eliminazione di Dr.Web Enterprise Server per i SO della famiglia UNIX® **95**

2.7.4. Eliminazione del Proxy **97**

**Capitolo 3. Componenti di rete antivirus e la loro interfaccia 99**

**3.1. Dr.Web Enterprise Server 99**

**3.2. Dr.Web Enterprise Agent 103**

**3.3. Centro gestione di Dr.Web 107**

3.3.1. Amministrazione **113**

3.3.2. Rete antivirus **115**

3.3.3. Impostazioni **121**

3.3.4. Legami **126**

3.3.5. Aiuto **127**

**3.4. Componenti Centro gestione Dr.Web 128**

3.4.1. Scanner di rete **128**

3.4.2. Manager licenze **133**

**3.5. Schema interazione componenti rete antivirus** **143**

## Capitolo 4. Inizio lavoro. Informazioni generali 149

**4.1. Creazione rete antivirus semplice** **149**

**4.2. Configurazione connessioni di rete** **152**

## Capitolo 5. Amministratori di rete antivirus 157

**5.1. Autenticazione di amministratori** **157**

**5.2. Tipi amministratori** **163**

**5.3. Gestione utenze amministratori** **164**

5.3.1. Creazione e eliminazione amministratori **165**

5.3.2. Modifica amministratori **167**

## Capitolo 6. Gruppi. Gestione complessa di workstation 169

**6.1. Gruppi di sistema e custom** **169**

**6.2. Gestione gruppi** **173**

6.2.1. Creazione e eliminazione gruppi **173**

6.2.2. Impostazioni di gruppi **175**

**6.3. Aggiungere workstation al gruppo. Eliminare workstation dal gruppo** **177**

**6.4. Utilizzo dei gruppi per impostare le workstation** **179**

6.4.1. Ereditarietà di elementi di configurazione di workstation. Gruppi primari **180**

6.4.2. Copiare le impostazioni in altri gruppi / workstation **183**

**6.5. Comparazione workstation e gruppi** **183**

## Capitolo 7. Gestione workstation 185

**7.1. Gestione record di workstation** **186**

7.1.1. Politica di connessione workstation **186**

7.1.2. Eliminazione e ripristino workstation **188**

**7.2. Configurazione workstation** **189**

7.2.1. Configurazione diritti utenti **195**

7.2.2. Visualizzazione componenti installati del pacchetto antivirus **197**

7.2.3. Contenuti pacchetto antivirus **199**

**7.3. Configurazione di Dr.Web Enterprise Agent per il SO Windows®** **200**

**7.4. Configurazione orario processi su workstation** **206**

**7.5. Scansione antivirus di workstation** **211**

7.5.1. Visualizzazione e arresto del funzionamento di componenti avviati **212**

7.5.2. Arresto funzionamento componenti avviati per tipi **212**

7.5.3. Avvio scansione workstation **213**

7.5.4. Configurazione parametri Scanner per SO Windows® **215**

**7.6. Visualizzazione risultati di operazione e statistiche consuntivi per workstation** **226**

7.6.1. Tabelle **227**

7.6.2. Grafici **232**

7.6.3. Informazioni libere **235**

7.6.4. Quarantena **236**

**7.7. Impostazioni di alcuni componenti antivirus** **238**

7.7.1. Configurazione di Controllo Ufficio per accedere alle risorse locali e di rete nel SO Windows® **239**

7.7.2. Configurazione del componente MailD per protezione di indirizzi di posta nei SO UNIX® e Mac OS X **241**

**7.8. Invio messaggi all'utente** **241**

**Capitolo 8. Configurazione di Dr.Web Enterprise Server** **247**

**8.1. Configurazione di Dr.Web Enterprise Server** **247**

8.1.1. Utilizzo di codifica e compressione traffico **256**

8.1.2. Configurazione modalità operazione con database **258**

8.1.3. Configurazione avvisi **261**

**8.2. Gestione del log di server** **263**

**8.3. Configurazione orario di Dr.Web Enterprise Server** **264**

**8.4. Gestione repositorio di Dr.Web Enterprise Server** **268**

8.4.1. Introduzione **268**

8.4.2. Stato del repository **269**

8.4.3. Editor configurazioni del repository **270**

**8.5. Particolarità di rete con più server di Dr.Web Enterprise Server** **273**

8.5.1. Struttura di rete con più Dr.Web Enterprise Server **273**

8.5.2. Configurazione comunicazioni intra-server tra Dr.Web Enterprise Server **276**

8.5.3. Utilizzo di rete antivirus con più Dr.Web Enterprise Server **284**

8.5.4. Operazione di più Server Dr.Web Enterprise Server con database unico **286**

## Capitolo 9. Aggiornamento di Dr.Web Enterprise Security Suite e di componenti singoli **287**

**9.1. Aggiornamento di Dr.Web Enterprise Security Suite** **287**

9.1.1. Aggiornamento di Dr.Web Enterprise Server per i SO Windows® **287**

9.1.2. Aggiornamento di Dr.Web Enterprise Server per i SO della famiglia UNIX® **294**

9.1.3. Aggiornamento di plug-in Dr.Web Browser-Plugin **302**

9.1.4. Aggiornamento di Dr.Web Enterprise Agent 303
9.1.5. Aggiornamento di Proxy 303
**9.2. Aggiornamento manuale dei componenti di Dr.Web Enterprise Security Suite 305**
**9.3. Aggiornamento programmato 307**
**9.4. Aggiornamento repositorio Dr.Web Enterprise Server, non connesso a Internet 309**
**9.5. Limitazione di aggiornamenti di workstation 311**
**9.6. Aggiornamento di Agent mobili Dr.Web Enterprise Agent 312**
**9.7. Aggiornamento di chiave di server e di chiave di workstation 314**
**Capitolo 10. Configurazione dei componenti supplementari 317**
**10.1. Server proxy 317**
**10.2. NAP Validator 322**
**Allegati 326**
**Allegato A. Lista completa delle versioni supportate dei SO 326**
**Allegato B. Configurazioni, necessarie per utilizzo di DBMS. Configurazioni driver DBMS 333**
Allegato B1. Configurazione driver ODBC 336
Allegato B2. Configurazione driver database per Oracle 338
Allegato B3. Configurazione database driver per SQL CE 342
Allegato B4. Utilizzo di DBMS PostgreSQL 345
**Allegato C. Descrizione parametri sistema di avvisi 348**
**Allegato D. Parametri modelli sistema di avvisi 349**
**Allegato E. Specifica di indirizzo di rete 357**
E1. Formato generale di indirizzo 357

E2. Indirizzi di Dr.Web Enterprise Server **360**

E3. Indirizzi di Dr.Web Enterprise Agent/ Installer **361**

**Allegato F. Gestione repositorio** **363**

F1. Sintassi di file di configurazione .config **364**

F2. Significato istruzioni del file .config **366**

F3. File .id **372**

F4. Esempi gestione repositorio con modifica del file di stato **373**

**Allegato G. File di configurazione** **375**

G1. File di configurazione di Dr.Web Enterprise Server **375**

G2. File di configurazione del Centro gestione di Dr.Web **384**

G3. File di configurazione download.conf **388**

G4. File di configurazione del server proxy **389**

**Allegato H. Parametri riga di comando di programmi, che fanno parte di Dr.Web Enterprise Security Suite** **394**

H1. Introduzione **394**

H2. Plugin di interfaccia di Dr.Web Enterprise Agent **395**

H3. Dr.Web Enterprise Agent **396**

H4. Installazione di rete **400**

H5. Dr.Web Enterprise Server **403**

H6. Utilità di amministrazione del database incorporato **417**

H7. Utilità di generazione di copie di chiavi e di firma digitale **418**

H8. Gestione Server Dr.Web Enterprise Server nei SO della famiglia UNIX® con il comando kill **419**

H9. Scanner Dr.Web per il SO Windows® **419**

H10. Server proxy **420**

**Allegato I. Variabili di ambiente, esportate da Server Dr.Web Enterprise Server** **422**

**Allegato J. Utilizzo di script di installazione iniziale per Dr.Web Enterprise Agent** **423**

**Allegato K. Utilizzo di espressioni regolari in Dr.Web Enterprise Security Suite** **428**

K1. Opzioni di espressioni regolari **428**

K2. Particolarità delle espressioni regolari PCRE **430**

**Allegato L. Formato dei file del log** **433**

**Allegato M. Descrizione di procedure dell'utente** **436**

**Allegato N. Integrazione XML Web API e Dr.Web Enterprise Security Suite** **440**

**Allegato O. Procedure di autenticazione degli amministratori** **441**

**Allegato P. Licenze** **446**

P1. Boost **447**

P2. Curl **448**

P3. Libradius **449**

P4. MD5 implementation **450**

P5. Net-snmp **451**

P6. OpenLDAP **460**

P7. OpenSSL **462**

P8. Oracle Instant Client **466**

P9. PCRE **474**

P10. Sha2 implementation **477**

P11. Wtl **479**

P12. Zlib **486**

P13. MIT License **487**

P14. GNU General Public License **488**

P15. GNU Lesser General Public License **505**

P16. Mozilla Public License 509

**FAQ 520**

**Trasporto di Dr.Web Enterprise Server su altro computer (nel SO Windows®) 520**

**Connessione di Agent Dr.Web Enterprise Agent ad un altro Dr.Web Enterprise Server 523**

**Cambio tipo DBMS di Dr.Web Enterprise Security Suite 525**

**Ripristino del database di Dr.Web Enterprise Security Suite 530**

**Ripristino di Dr.Web Enterprise Server dal backup dei dati 537**

**Aggiornamento di Agent sui server LAN 541**

**Ripristino della password di amministratore Dr.Web Enterprise Security Suite 542**

**Utilizzo di DFS durante l'installazione di Agent via Active Directory 544**

**Rilevamento dei problemi di installazione remota 545**

**Indice analitico 548**

# Capitolo 1. Introduzione

## 1.1. Introduzione

Nel presente Manuale si contengono le informazioni che descrivono sia principi comuni, sia particolari di realizzazione della protezione antivirus complessa dei computer della società con **Dr.Web® Enterprise Security Suite** (di seguito brevemente denominato **Dr.Web ESS**). Nel manuale non vengono descritti i pacchetti antivirus di **Dr.Web** per i computer protetti. Per le informazioni corrispondenti v. il manuale **Dr.Web® Anti-virus per Windows. Manuale dell'utente.**

Il presente Manuale è disegnato per *amministratore della rete antivirus* — dipendente della società, a cui è affidata la gestione della protezione antivirus dei computer (workstation e server) di tale rete.

Amministratore della rete antivirus deve avere le autorizzazione dell'amministratore di sistema o collaborare con l'amministratore della rete locale, essere competente nella strategia della protezione antivirus e conoscere in dettagli i pacchetti antivirus di **Dr.Web** per tutti i SO utilizzati nella rete.

Alcuni capitoli iniziali del Manuale saranno utili per il responsabile della società che prende la decisione di acquisto e di installazione del sistema della protezione antivirus complessa.

L'ultima parte del documento (Allegati) contiene le informazioni tecniche che descrivono i parametri necessari per la configurazione dei componenti Antivirus, nonché la sintassi e i valori di istruzioni, utilizzate per lavorare con essi.

Prima di leggere il documento assicurarsi che sia l'ultima versione del **Manuale dell'Amministratore**. Il manuale viene aggiornato in continuazione, l'ultima versione può sempre essere reperita sul sito ufficiale della società **Doctor Web** http://download.drweb.com/esuite/.

# 1.2. Segni convenzionali e abbreviazioni

## Segni convenzionali

Nel presente Manuale vengono utilizzati i segni, riportati nella tabella 1-1.

**Tabella 1-1. Segni convenzionali**

| Segno | Commento |
|---|---|
|  Nota bene | Indicazione o osservazione importante. |
|  Attenzione | Avviso di eventuali situazioni di errori, nonché dei momenti importanti, a cui particolarmente prestare attenzione. |
| **Dr.Web ESS** | Denominazioni dei prodotti e dei componenti di **Dr.Web**. |
| *Rete antivirus* | Termine nella posizione di definizione o di collegamento a definizione. |
| *<indirizzo-IP>* | Campi per sostituire le denominazioni funzionali con i valori attuali. |
| **Annullare** | Denominazioni di tasti dello schermo, di finestre, di voci del menu e di altri elementi dell'interfaccia di programma. |
| CTRL | Denominazione dei tasti della tastiera. |
| `C:\Windows\` | Denominazioni dei file e delle cartelli, dei frammenti di codice del programma. |
| Allegato A | Riferimenti incrociati a capitoli del documento o collegamenti ipertestuali alle risorse interne. |

## Abbreviazioni

Nel testo del Manuale vengono utilizzate le seguenti abbreviazioni senza spiegazione:

- ACL – lista di controllo degli accessi (Access Control List),
- DFS – file system distribuito (Distributed File System),
- **Dr.Web ESS** – **Dr.Web Enterprise Security Suite**,
- GUI – interfaccia grafica utente (Graphical User Interface), GUI-versione del programma — versione che utilizza strumenti di GUI,
- NAP – Network Access Protection,
- UDS – UNIX Domain Socket (socket di dominio UNIX),
- DB, DBMS – database, database management system,
- **SAM Dr.Web** – sistema aggiornamenti mondiale di **Dr.Web**,
- LAN – rete in area locale,
- SO – sistema operativo,
- EBNF – Extended Backus-Naur form.

# 1.3. Contenuti, destinazione e funzionalità principali di Dr.Web Anti-virus Enterprise Security Suite

Anti-virus **Dr.Web Enterprise Security Suite** è sviluppato per organizzazione e gestione della protezione antivirus unica ed affidabile di complesso dei computer della società. Non è necessario che i computer siano uniti nella rete locale, è sufficiente accesso a Internet.

***Dr.Web Enterprise Security Suite risolve i seguenti compiti:***

- installazione centralizzata (senza necessità di accesso diretto del personale) di pacchetti antivirus su computer protetti,
- configurazione centralizzata dei parametri di pacchetti antivirus,
- aggiornamento centralizzato dei database dei virus e del

software su computer protetti,

- monitoraggio di eventi dei virus, nonché dello stato dei pacchetti antivirus e dei SO su tutti i computer protetti.

**Dr.Web ESS** permette sia di lasciare a utenti di computer protetti i diritti di configurare e di gestire pacchetti antivirus di tali computer, sia di limitarli flessibilmente, fino al divieto completo.

Rete antivirus **Dr.Web ESS** ha architettura di tipo *client-server*. I suoi componenti si installano su computer di utenti, di amministratori e su computer, che esegue/eseguono le funzionalità di **Enterprise Server**, e si scambiano le informazioni, utilizzando i protocolli di rete TCP/IP, IPX/SPX, NetBIOS. L'insieme dei computer, su cui sono installati i componenti interagenti di **Dr.Web ESS**, viene chiamato *rete antivirus*.

### *I seguenti componenti fanno parte della rete antivirus:*

**Componenti principali:**

- *Dr.Web Enterprise Server (Enterprise Server)*. Questo componente viene installato su uno dei computer della rete antivirus. Conserva le distribuzioni dei pacchetti antivirus per i vari SO dei computer protetti, gli aggiornamenti di database dei virus, dei pacchetti antivirus e di **Enterprise Agent**, le chiavi di utenti e le impostazioni dei pacchetti dei computer protetti e li passa su richiesta di **Enterprise Agent** a computer corrispondenti. **Enterprise Server** gestisce il log unico di eventi della rete antivirus.
- *Centro gestione Dr.Web*. Questo componente viene installato automaticamente insieme a **Enterprise Server**. È un'estensione di pagina web e permette di gestire la rete antivirus in remoto, modificando le impostazioni di **Enterprise Server**, nonché le impostazioni dei computer protetti, salvati su **Enterprise Server** e su computer protetti.

- *Dr.Web Enterprise Agent (Enterprise Agent)*. Questo componente viene installato su computer protetto, dopodiché ci esegue l'installazione del pacchetto antivirus. Di seguito **Enterprise Agent** esegue aggiornamenti regolari del software antivirus installato, gli passa i comandi e le impostazioni da **Enterprise Server**, e inoltre spedisce a **Enterprise Server** le informazioni su eventi dei virus ed altre informazioni necessarie del computer protetto.

**Componenti supplementari:**

- *Server proxy*. Questo componente può opzionalmente essere incluso nella struttura di una rete antivirus. Il compito principale del **Server proxy** – assicurare la connessione di **Enterprise Server** e di **Enterprise Agent** nel caso non sia possibile organizzare accesso diretto, per esempio, se **Enterprise Server** e **Enterprise Agent** sono situati nelle reti diverse, tra cui non c'è il routing dei pacchetti. Per via di utilizzo della funzionalità di caching si può diminuire l'utilizzo del traffico di rete e il tempo di ottenimento aggiornamenti di **Enterprise Agent**.
- *NAP Validator.* Permette di utilizzare la tecnologia *Microsoft Network Access Protection (NAP)* per controllare l'operabilità del software di workstation protette in base alla corrispondenza alle policy.



**Enterprise Server** può essere installato su qualsiasi computer, oltre il computer che esegue le funzioni di server LAN. I requisiti principali di tale computer sono riportati in Requisiti di sistema.

**Centro gestione** e **Server** possono essere installati su diversi computer. Devono solamente essere connessi.

Rete antivirus può includere più **Enterprise Server**. Particolarità di tale configurazione sono descritte in Particolarità di rete con più server antivirus.

***I seguenti componenti fanno parte del pacchetto antivirus di Dr.Web, installato su workstation protette:***

**Componenti principali:**

- *Dr.Web Scanner per Windows* fa parte del prodotto standard **Dr.Web per Windows**. Le impostazioni di scanner vengono configurate direttamente per esso (via le impostazioni del gruppo o via impostazioni personalizzate per workstation). Controlla PC a richiesta dell'utente o secondo orario locale dell'utente. Inoltre include il modulo antirootkit.
- *Dr.Web Enterprise Scanner per Windows* è una delle funzionalità di **Enterprise Agent**. Anch'esso è uno scanner antivirus che utilizza gli stessi database dei virus che il nucleo di ricerca. Comunque la funzionalità è "incorporata" in **Enterprise Agent**. Destinazione di **Dr.Web Enterprise Scanner per Windows** - eseguire la scansione antivirus a richiesta: o dall'avvio programmato, o dal compito diretto **Scansionare** dal **Centro gestione Dr.Web**. Non ha nessuna interfaccia speciale né impostazioni di operazione autonome, tutto viene impostato solamente via il **Centro gestione** all'avvio di **Scanner** (alla configurazione di avvio programmato o all'iniziazione manuale della scansione).
- *Monitoraggio di sistema SelfPROtect* fornisce la protezione dei file e delle cartelle di **Dr.Web ESS** da eliminazione non autorizzata o casuale o dalla modifica da utente, nonché dal software dannoso. Quando monitoraggio di sistema è attivato, l'accesso alle risorse indicate è consentito solamente ai programmi di **Dr.Web**.

**Componenti supplementari:**

- *SpIDer Guard (monitoraggio di file)* risiede continuamente nella memoria e controlla "al volo" tutti i file aperti su dischi rimovibili e i file su dischi rigidi, aperti per il salvataggio. Oltre questo, la guardia costantemente monitora le azioni dei processi avviati, tipici per virus, e al loro rilevamento blocca i processi, visualizzandone un avviso corrispondente all'utente.
- *SpIDer Mail (monitoraggio di posta)* anch'esso risiede continuamente nella memoria. Il programma intercetta tutti i richiami di client di posta del PC dei server di posta tramite i

protocolli POP3/SMTP/IMAP4/NNTP e controlla tutta la posta in entrata (in uscita) prima che il client di posta la riceva (o la invii).

- *SplDer Gate* (*monitoraggio HTTP)* risiede continuamente nella memoria del computer e intercetta tutti i richiami dei siti web tramite il protocollo HTTP. Il programma neutralizza le minacce nel traffico HTTP (per esempio, nei file spediti o ricevuti), nonché blocca accesso a risorse sospette o non corrette.
- *Dr.Web Controllo Ufficio* risiede continuamente nella memoria del computer e - se sono presenti le impostazioni corrispondenti - gestisce accesso alle risorse di rete e alle risorse locali indicate. In particolare, il componente permette di controllare accesso ai siti web, consentendo o bloccando a utenti la frequentazione di certi nodi della rete Internet. Il programma permette non solamente di controllare l'integrità di file importanti da modifiche occasionali o da infezione con virus, ma blocca a dipendenti accesso alle informazioni indesiderate.
- *Dr.Web FireWall* è destinato per proteggere il computer da accesso non autorizzato dall'esterno e per prevenire la fuga dei dati importanti in Internet. Il componente permette di controllare le connessioni e la trasmissione dei dati in Internet e di bloccare le connessioni sospette al livello dei pacchetti e di applicazioni.

## 1.4. Vantaggi

- Software del server multipiattaforma, che permette di utilizzare come **Enterprise Server** sia i computer con i SO Microsoft® Windows®, sia i computer con i SO della famiglia UNIX®.
- Software di agent multipiattaforma, che permette di eseguire la protezione antivirus dei computer con i SO della famiglia Microsoft Windows, Android, Microsoft® Windows Mobile®, Novell® NetWare®, con i SO della famiglia UNIX, Mac OS X.
- Protezione antivirus del sistema di posta Microsoft® Outlook® e dei sistemi di posta, costruiti sulla base di server IBM® Lotus® Domino® o Microsoft® Exchange Server.
- Traffico di rete minimo di reti locali, costruiti sulla base di protocolli TCP/IP, IPX e NetBIOS, con possibilità di applicare

algoritmi speciali di compressione.

- Possibilità di codificare i dati scambiati tra i vari componenti di sistema.
- Gestione semplificata di workstation della rete antivirus per via di utilizzo dei gruppi.
- Possibilità di gestire protezione antivirus (via **Centro gestione** di **Dr.Web**) praticamente da ogni computer con qualsiasi SO.
- Possibilità di installazione remota e di eliminazione dei componenti del pacchetto dall'amministratore di sistema direttamente via **Centro gestione.**
- Installazione centralizzazata di **Enterprise Agent** (con possibilità di configurare il software di **Enterprise Agent** su **Enterprise Server** prima di installarlo su computer client).
- Possibilità di utilizzare filtro spam su workstation antivirus (a condizione che la licenza acquistata permetta di utilizzare tale funzionalità).
- Distribuzione veloce ed efficace dal **Server** di aggiornamenti di database dei virus e di plug-in a workstation protette.
- Funzionalità di creazione di copie di riserva dei dati critici del **Server** (database, file di configurazione ecc).



A differenza di altri prodotti antivirus, **Dr.Web ESS Antivirus** può essere installato anche su computer infetti di utenti.

## 1.5. Requisiti di sistema

***Per l'installazione e il funzionamento di Dr.Web ESS si richiede:***

- che **Enterprise Server** sia installato sul computer, che ha accesso a Internet, per ricevere aggiornamenti automaticamente dai server **SAM** (Sistema aggiornamenti mondiale) di **Dr.Web**;
- che i computer della rete antivirus abbiano accesso a Internet per connettersi a **Enterprise Server** o a **Server** o che siano nella stessa rete locale;

- per il funzionamento comune di componenti antivirus su computer utilizzati devono essere aperti tutte le porte e tutti i socket necessari:

| Numero | Protocollo | Destinazione |
|---|---|---|
| porta 2193, 2371 | TCP, UDP | Per connessione di componenti antivirus al **Server**. |
| socket 2371 | IPX/SPX | Per connessione di componenti antivirus al **Server**. |
| porte 2193, 2372 | UDP | Per operazione di Scanner di rete. |
| porte 139, 445 | TCP, UDP | Per operazione di **Installazione di rete**. |
| porta 9080 | http | Per operazione di Centro gestione Dr.Web. |
| porta 9081 | https | Per operazione di Centro gestione Dr.Web. |



La porta 2371 è necessaria per comunicazione (via protocolli TCP e UDP) con componenti della versione **4.XX**. Si utilizza per provvedere alla compatibilità, in particolare, nel processo di aggiornamento dei componenti della rete antivirus.

***Per il funzionamento di Dr.Web Enterprise Server si richiedono:***

- processore Intel® Pentium® III con frequenza di 667 MHz e superiore,
- memoria operativa 512 MB (1 GB se si utilizza il database incorporato),
- memoria libera (disponibile) sul disco rigido fino a 12 GB: fino a 8 GB per il database incorporato (cartella di installazione), fino a 4 GB nella cartella temporanea di sistema (per i file operativi),



Durante l'installazione del **Server** è necessario che sul disco di sistema (nonostante dove è installato il **Server** stesso) ci siano non meno di 2,5 GB della memoria libera per la distribuzione completa o 650 MB per la distribuzione alleggerita - per avviare l'installazione e decomprimere i file temporanei.

- SO Windows 2000 e superiori, SO Linux®, SO FreeBSD® o SO Solaris™ (v. Allegato A. Lista completa delle versioni supportate dei SO),
- all'installazione di **Enterprise Server** per i SO della famiglia UNIX si richiede la presenza di librerie: `libiconv` della versione `1.8.2` o superiore, `pcre`, `ncurses`, `openssl`, `libcrypto` e `libssl` (librerie condivise, di solito incluse in `openssl`), `libxml2`, `libpq` (solo per l'utilizzo con il database **PostgreSQL**; all'installazione via pacchetti generic, la libreria già ne fa parte), `libcurl` della versione `7.20.0` e superiori, `libldap`.

***Per operazione del server proxy si richiedono:***

- processore Intel Pentium III con frequenza di 667 MHz e superiore,
- memoria operativa non meno di 512 MB,
- memoria libera (disponibile) sul disco rigido: non meno di 1 GB,
- SO Windows 2000 e superiore, SO Linux, SO FreeBSD o SO Solaris (simili a **Enterprise Server**, v. Allegato A. Lista completa delle versioni supportate dei SO),
- all'installazione del **Server proxy** nei SO della famiglia UNIX si richiede la presenza di librerie: `libiconv` della versione `1.8.2` e superiori, `pcre`, `libxml2`.



Si può scaricare la libreria `libiconv` dal server ftp://ftp.freebsd.org.

***Per operazione di NAP si richiedono:***

**Per server:**

- SO Windows Server 2008.

**Per agent:**

- SO Windows XP SP3, SO Windows Vista, SO Windows Server 2008.

***Per operazione del Centro gestione Dr.Web si richiedono:***

- Browser web Windows® Internet Explorer® 7 e superiori o browser web Mozilla® Firefox® 3.0 e superiori.



Si possono inoltre utilizzare i browser web Opera® 10 e superiori, Safari® 4 e superiori, Chrome® 7 e superiore. Comunque la possibilità di operazione in questi browser web non è garantita.

All'installazione del **Server** sul computer, in cui nome è presente il carattere "_" (trattino basso), operazione con **Server** via **Centro gestione** nel browser Windows Internet Explorer non sarà possibile.

In questo caso si deve utilizzare altro browser web.

Per una corretta operatività del **Centro gestione** nel browser Windows Internet Explorer, l'indirizzo IP e/o il nome DNS del computer, su cui è installato **Enterprise Server**, devono essere inseriti tra i siti attendibili del browser, in cui si usa il **Centro gestione**.

Per aprire il **Centro gestione** in modo corretto tramite il menu **Start**, se si usa il browser Windows Internet Explorer nei SO Windows 8 e Windows Server 2012 basati sull'interfaccia delle piastrelle dinamiche, è necessario impostare i seguenti parametri del browser: **Opzioni Internet** → **Programmi** → **Apertura di Internet Explorer** spuntare il flag **Sempre in Internet Explorer in visualizzazione classica**.

- Plug-in **Dr.Web Browser-Plugin** per operazione completa con

**Centro gestione**. Plugin viene fornito insieme alla distribuzione del **Server** e viene installato a richiesta del browser nel processo di operazione con elementi del **Centro gestione**, che richiedono di caricare il plugin (per **Scanner di rete**, alla installazione remota dei componenti antivirus).



Per operazione del plug-in **Dr.Web Browser-Plugin** sulla pagina dello **Scanner di rete** sia nei SO Windows, sia nei SO della famiglia GNU/Linux, sono richiesti i diritti dell'amministratore (root).

Se si utilizza il browser web Safari, il plugin **Dr.Web Browser-Plugin** è disponibile solo per le versioni, che operano nei SO Windows.

Con utilizzo dei browser web Mozilla Firefox, Opera e Chrome il plugin **Dr.Web Browser-Plugin** è disponibile solo per le versioni, che operano nei SO Windows e nei SO della famiglia Linux.

- Risoluzione dello schermo consigliabile per operazione del **Centro gestione** 1280x1024 pt.

***Per operazione di Dr.Web Enterprise Agent e del completo pacchetto antivirus si richiede:***

1. Requisiti minimi:
   - processore Intel Pentium IV con frequenza di 1.6 GHz;
   - memoria operativa 512 MB.
2. Requisiti consigliabili:
   - processore Intel Pentium IV con frequenza di 2.4 GHz e superiore;
   - memoria operativa non meno di 1 GB.
3. Spazio libero su disco fisso: non meno di 250 MB per i file eseguibili + in più per i protocolli di operazione e per i file temporanei;
4. Sistemi operativi (v. Allegato A. Lista completa delle versioni supportate dei SO):
   a) SO Windows 98, SO Windows Me, SO Windows NT4 (SP6) e superiori. In questo caso, a seconda del SO, si possono installare i seguenti componenti:

| Componente | SO |
|---|---|
| **SpIDer Gate**, **SelfPROtect**, **Controllo Ufficio**, **Dr.Web Browser-Plugin per Outlook** | Windows 2000 con SP4 e superiori. |
| **SpIDer Guard NT4**, **Dr.Web Scanner NT4** | • Windows 98,<br>• Windows ME,<br>• Windows NT4 (SP6a),<br>• Windows 2000 con SP4 senza Update Rollup1,<br>• Windows XP senza SP, ed anche con SP1,<br>• Windows 2003 senza SP. |
| **FireWall**, **SpIDer Guard G3**, **Dr.Web Scanner** | • Windows 2000 con SP4 e Update Rollup1,<br>• Windows XP con SP2 e superiori,<br>• Windows 2003 con SP1 e superiori,<br>• Windows Vista e superiori. |
| **SpIDer Mail NT4** | • Windows 98,<br>• Windows NT4 con SP6a. |
| **SpIDer Mail** | Tutti i SO supportati, superiori ai sistemi per la versione **SpIDer Mail NT4**. |

b) SO Microsoft® Windows Mobile®;

c) SO Novell NetWare;

d) SO della famiglia UNIX: SO Linux, SO FreeBSD o SO Solaris;

e) SO Android;

f) Mac OS X.

5. Plug-in **Dr.Web per Outlook** richiede il client installato Microsoft Outlook di MS Office:

- Outlook 2000 (Outlook 9),
- Outlook 2002 (Outlook 10 o Outlook XP),
- Office Outlook 2003 (Outlook 11),
- Office Outlook 2007,
- Office Outlook 2010.

6. Per il funzionamento corretto della guida contestuale **Dr.Web Agent per Windows** è richiesto Windows Internet Explorer 6.0 e superiori.



Su workstation della rete antivirus, gestita con **Dr.Web Enterprise Security Suite**, non si deve utilizzare altro software antivirus (compreso software di altre versioni dei programmi antivirus di **Dr.Web**).



Le funzionalità dell'**Agent** nel SO Windows Mobile e Novell NetWare sono descritte nei manuali dell'utente **Dr.Web Agent per Windows Mobile** e **Dr.Web Agent per Novell NetWare**.

# 1.6. Set di fornitura

***Distribuzione di Dr.Web Enterprise Security Suite viene fornita in due varianti a secondo il SO del Enterprise Server scelto:***

1. Per installazione nei SO della famiglia UNIX – come file nel formato di archivio `bzip2` o pacchetti di installazione per la versione corrispondente del SO di seguenti componenti:
   - **Dr.Web Enterprise Server**,
   - **Server proxy**.
2. Per installazione nei SO Windows — come file eseguibili di installazione guidata per i seguenti componenti:
   - **Dr.Web Enterprise Server**,
   - **Server proxy**,
   - **Dr.Web Enterprise Agent** per Active Directory,
   - **NAP Validator**.

***Distribuzione di Enterprise Server viene fornita in due varianti:***

1. *Distribuzione completa* - comprende le distribuzioni di tutti i prodotti corporativi, forniti per installazione su workstation protette, gestite da tutti i SO supportati.
2. *Distribuzione alleggerita* - distribuzione, la cui composizione è analoga alla composizione di distribuzione delle versioni precedenti di **Dr.Web Enterprise Security Suite**.

   Conviene all'installazione di protezione antivirus, gestita da **Dr.Web Enterprise Security Suite**, sulle workstation solamente con i SO Windows.

***Nella distribuzione di Enterprise Server sono compresi i seguenti componenti:***

- software di **Dr.Web Enterprise Server** per il SO corrispondente,
- software di **Agent Dr.Web Enterprise Agent** e di pacchetti antivirus per i SO supportati,

- software del **Centro gestione Dr.Web**,
- database dei virus,
- documentazione, moduli e esempi.

Oltre la distribuzione stessa vengono forniti anche i numeri di serie, dopo la cui registrazione si ottengono i file con chiave del server e chiave per le workstation.

## 1.7. File chiavi

I diritti di utilizzo di **Dr.Web Enterprise Security Suite** vengono regolati via i seguenti file chiavi:

1. File chiave per **Server** - `enterprise.key`.
2. File chiave per le workstation - `agent.key`.



Il file della chiave ha il formato, protetto dalle modifiche con il meccanismo di firma digitale. La modifica del file lo rende non valido. Per evitare che si daneggi casualmente, non si deve modificare il file della chiave e/o salvarlo dopo la sua visualizzazione in editor di testo.

Contenuti e costo della licenza di utilizzo della soluzione antivirus di **Dr.Web ESS** dipendono dal numero di workstation protette nella rete (compresi i server che fanno parte della rete di **Dr.Web ESS** come workstation protette).



Questa informazione si deve obbligatoriamente comunicare al rivenditore licenza all'acquisto della soluzione **Dr.Web ESS**. Si deve inoltre indicare il numero di **Enterprise Server**, necessari per creare rete antivirus. Numero di **Enterprise Server** utilizzati indipendenti (non connesse l'uno con l'altro) non comporta l'aumento del costo della licenza (v. anche Creazione rete antivirus).



Da segnalare, che alla creazione di una rete antivirus con più **Server** (v. Particolarità di rete con più server), quando si calcolano le workstation protette si devono considerare le comunicazioni di **Enterprise Server**, siccome tali comunicazioni richiedono una licenza supplementare. In questo caso, per ogni **Enterprise Server** ogni comunicazione intraserver, nonostante il suo tipo (v. Struttura di rete con più server) richiede licenza separata, siccome alla comunicazione di due **Server** serve una licenza supplementare di comunicazione intraserver per tutti e due.

File chiavi di licenza possono fare parte del set antivirus di **Dr.Web ESS** all'acquisto. Comunque, di solito vengono forniti solamente i numeri di serie.

File chiavi di licenza vengono inviati a utenti per posta elettronica, di solito, dopo la registrazione del numbero di serie su un sito web speciale (indirizzo del sito della registrazione http://products.drweb.com/register/, se l'altro indirizzo non è segnato nella scheda di registrazione, fornita insieme al prodotto). Entrare nel sito indicato, completare il modulo con le informazioni su acquirente e inserire nel campo indicato il numero di serie di registrazione (si trova sulla scheda di registrazione). Archivio con i file chiavi verrà inviato all'indirizzo indicato. Può inoltre essere scaricato direttamente dal file indicato.

File chiavi vengono forniti all'utente nell'archivio zip, che contiene i file chiavi per **Server** e workstation.

***Utente può ottenere i file chiavi in uno dei seguenti modi:***

- via posta elettronica (di solito dopo la registrazione sul sito web, v. sopra);
- insieme alla distribuzione del prodotto, se i file di licenza sono stati inclusi nella distribuzione alla sua integrazione;
- su dispositivo separato come file.

Si consiglia di conservare il file chiave di licenza fino alla scadenza del periodo della sua validità ed utilizzarlo alla reinstallazione o al ripristino dei componenti del programma. Se si perde il file della chiave di licenza, la procedura di registrazione può essere rifatta sul sito indicato

e si può ottenere di nuovo il file chiave di licenza. In questo caso si deve indicare lo stesso numero di serie di registrazione e le stesse informazioni su acquirente che durante la prima registrazione; può cambiare solamente l'indirizzo di posta elettronica. In questo caso il file chiave di licenza verrà inviato al nuovo indirizzo.

Per provare antivirus si possono utilizzare i file della chiave demo. Tali file della chiave forniscono le funzionalità complete di componenti antivirus principali, però hanno il periodo di validità limitato. Per ottenere i file della chiave demo, si deve compilare il modulo, che si trova sulla pagina http://download.drweb.com/demoreq/. La sua richiesta verrà analizzata individualmente. Nel caso di decisione positiva l'archivio con i file chiave verrà inviato all'indirizzo indicato.

Utilizzo dei file chiavi ottenuti nel processo di installazione del programma viene descritto in Installazione di Dr.Web Enterprise Server

Utilizzo dei file chiavi per una rete antivirus già effettiva è descritto in Aggiornamento della chiave server e chiave workstation.

# Capitolo 2. Installazione e eliminazione dei componenti di Dr.Web Enterprise Security Suite

## 2.1. Creazione rete antivirus

***Per creare una rete antivirus:***

1. Preparare lo schema della struttura di rete antivirus, includendoci tutti i computer protetti e definendo, quali di essi assumeranno la funzione di **Enterprise Server**.
2. Installare il software di **Enterprise Server** (insieme ad esso viene installato il **Centro gestione Dr.Web**) su una workstation scelta o sulle workstation.
3. Utilizzando il **Centro gestione**, eseguire l'aggiornamento del repositorio.
4. Configurare il software delle workstation e del **Server** (dei **Server**).
5. Se necessario, installare e configurare il **Server proxy**.
6. Installare il software di **Enterprise Agent** su workstation.



Appena installati su un computer, **Agent** stabiliscono automaticamente la connessione al **Server**. Autorizzazione di workstation antivirus su **Server** avviene a secondo la politica scelta (v. Politica connessione workstation).

7. Utilizzando **Centro gestione**, configurare ed avviare i plug-in richiesti.

Durante la fase di programmazione della struttura della rete antivirus prima di tutto si deve scegliere il computer che esegue le funzioni di **Enterprise Server**.



**Enterprise Server** può essere installato su qualsiasi computer, oltre il computer che esegue le funzioni di server LAN. I requisiti principali di tale computer sono riportati in Requisiti di sistema.

**Centro gestione** e **Server** possono essere installati su diversi computer. Devono solamente essere connessi.

Rete antivirus può includere più **Enterprise Server**. Particolarità di tale configurazione sono descritte in Particolarità di rete con più server antivirus.

Per installazione di **Enterprise Server** e di **Enterprise Agent** è necessario un accesso una volta sola (fisicamente o utilizzando strumenti di gestione remota e di avvio dei programmi) ai computer corrispondenti. Tutte le operazioni successive vengono eseguite da workstation dell'amministratore di rete antivirus (inclusa un'eventuale workstation, esterna alla rete locale) e non richiedono l'accesso a **Enterprise Server** o a workstation.

## 2.2. Installazione diDr.Web Enterprise Server

L'installazione di **Enterprise Server** è il primo passo della creazione della rete antivirus. Prima del suo completamento con successo non può essere installato nessun altro componente della rete antivirus.

L'avanzamento del processo di installazione di **Enterprise Server** dipende da quale versione del **Server** (per i SO Windows o per i SO della famiglia UNIX) viene installata. Comunque i contenuti dei parametri configurati nel processo di installazione e la struttura del software aggiornato corrispondono.



Tutti i parametri, impostati all'installazione, possono essere di seguito modificati dall'amministratore di rete antivirus nel processo del funzionamento del **Server**.

Se è già installato il software del **Server**, v. sezioni Aggiornamento di Dr.Web ESS per i SO Windows® o Aggiornamento di Dr.Web ESS per i SO della famiglia UNIX® rispettivamente.



Se prima di installare il software del **Server** è stata eseguita l'eliminazione del **Server**, installato in precedenza, durante l'installazione vengono eliminati i contenuti del repositorio e ne viene installata una versione nuova. Se per qualche motivo è rimasto il repositorio della versione precedente, si devono eliminare manualmente tutti i contenuti del repositorio prima di installare una versione nuova e si deve eseguire l'aggiornamento completo del repositorio dopo l'installazione del **Server**.

La lingua del nome della cartella, dove viene installato il **Server**, deve corrispondere alla lingua, indicata nelle impostazioni di lingua del SO Windows per i programmi, che non utilizzano Unicode. Nel caso contrario l'installazione del **Server** non viene avviata.

Eccezione – la lingua inglese nel nome della cartella di installazione.

Insieme a **Enterprise Server** viene automaticamente installato il **Centro gestione Dr.Web**, che serve per gestire la rete antivirus e per configurare il **Server**.

Di default **Enterprise Server** dopo l'installazione viene avviato automaticamente (per la versione nei SO della famiglia UNIX questo viene indicato nelle impostazioni del programma di installazione).

### 2.2.1. Installazione di Dr.Web Enterprise Server per i SO Windows®

Di seguito è descritta l'installazione di **Enterprise Server** per i SO Windows. Contenuti e conseguenza dei passi possono essere diversi a seconda della versione di distribuzione.

***Prima di installare Dr.Web Enterprise Server si consiglia di prestare attenzione alle seguenti informazioni:***



Se nel SO Windows sono installati servizi **Terminal Services**, l'installazione del software deve essere eseguita solo con il wizard **Programmi** del **Pannello di controllo** del SO Windows**.**

File di distribuzione ed altri file, richiesti durante l'installazione del programma, devono essere situati su dischi locali del computer, su cui viene installato il software del **Server**. I diritti di accesso deve essere configurati in modo che i file siano disponibili per utente **LOCALSYSTEM**.

Installazione di **Enterprise Server** deve essere eseguita dall'utente con i diritti dell'amministratore di tale computer.



Dopo l'installazione di **Enterprise Server** si deve eseguire l'aggiornamento di tutti i componenti di **Dr.Web ESS** (v. Aggiornamento manuale dei componenti di Dr.Web ESS).

Se si utilizza un database esterno, si deve creare prima il database e configurare il driver corrispondente (v. Allegato B. Impostazioni necessarie per utilizzare DBMS. Parametri dei driver DBMS).

In immagine 2-1. è riportato lo schema a blocchi del processo di installazione di **Enterprise Server** con programma di installazione. Suddivisione di installazione in passi corrisponde alla descrizione dettagliata della procedura, riportata sotto.

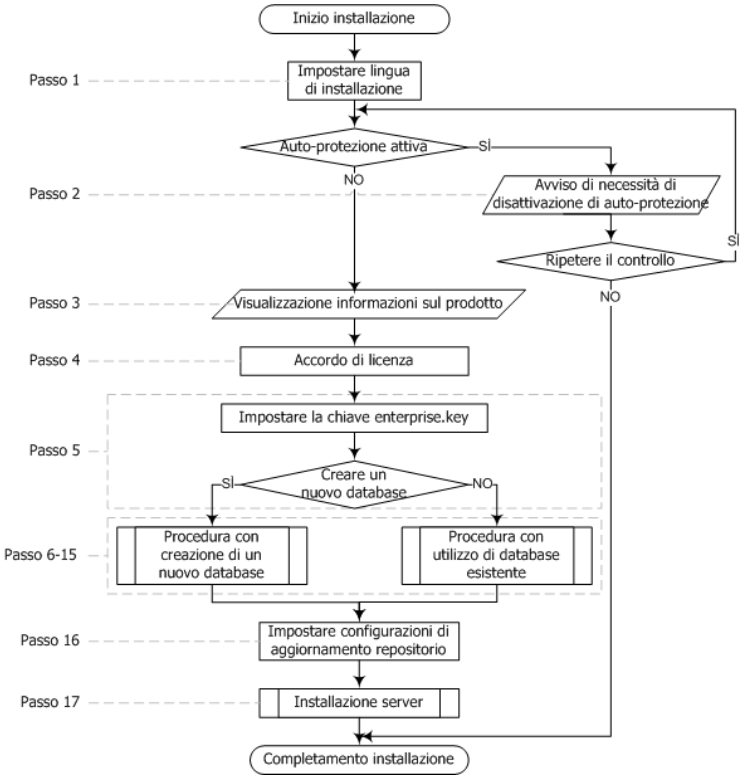



**Immagine 2-1. Lo schema del processo di installazione di Dr.Web Enterprise Server (Premere sul blocco di schema per passare alla descrizione)**

Lo schema a blocchi contiene tre procedure incorporate. La procedura **Installazione del Server** (passo 17) non richiede l'intervento dell'utente (v. descrizione sottostante) e viene eseguita direttamente dal programma di installazione.

Gli schemi a blocchi delle procedure **alla creazione di un database nuovo** e **all'utilizzo del database esistente** sono riportati in immagine 2-2. e immagine 2-3.

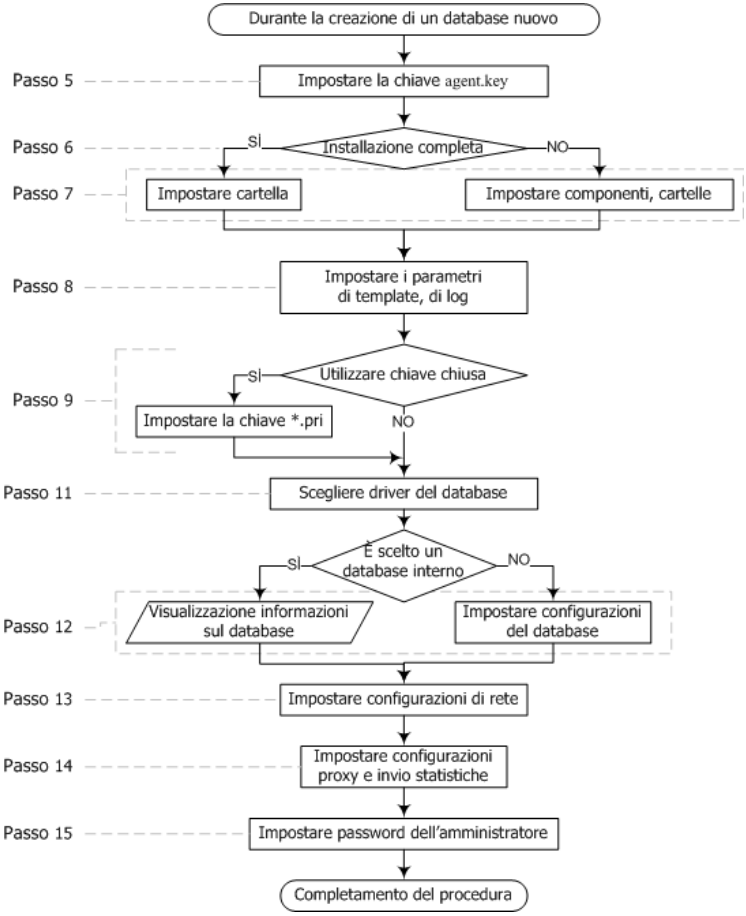



**Immagine 2-2. Lo schema della procedura di installazione alla creazione di un nuovo database (Premere sul blocco dello schema per passare alla descrizione)**

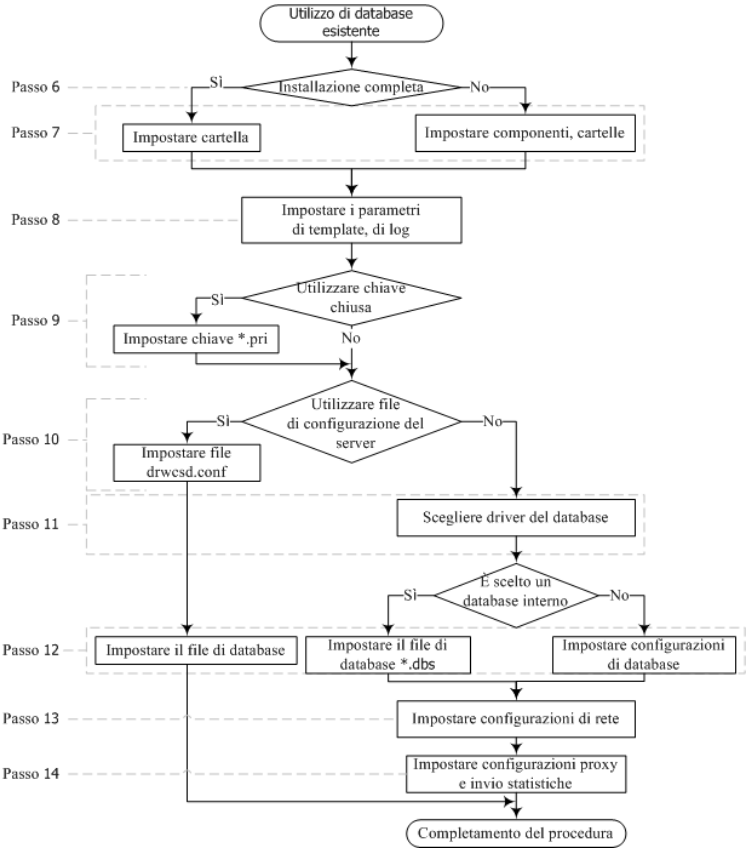



**Immagine 2-3. Lo schema della procedura di installazione di Dr.Web Enterprise Server con utilizzo del database esistente (Premere sul blocco dello schema per passare alla descrizione)**

### *Per installare Dr.Web Enterprise Server sul computer con il SO Windows:*

1. Avviare il file della distribuzione. Si apre la finestra di scelta della lingua, in cui verrà eseguita l'installazione successiva del prodotto. Scegliere **Italiano** e premere il tasto **Avanti**.
2. Di seguito, se sul computer con **Enterprise Server** è installato **Enterprise Agent** con autoprotezione attiva, verrà

visualizzato l'avviso che il componente di autoprotezione di **Dr.Web** è attivo. Disattivare tale componente via le impostazioni di **Agent** e premere sul tasto **OK** per procedere o sul tasto **Cancel** per annullare l'installazione del **Server**.

3. Si apre la finestra **InstallShield Wizard** con informazioni sul prodotto installato. Premere sul tasto **Avanti**.
4. Si apre la finestra con il testo dell'Accordo di licenza. Dopo aver letto i termini dell'accordo di licenza nel gruppo di tasti di scelta nella parte inferiore della finestra scegliere **Accetto i termini dell'accordo di licenza** e premere sul tasto **Avanti**.
5. Si apre la finestra di scelta dei file chiavi di licenza.

   Vicino al campo **Chiave per Dr.Web Enterprise Server** premere sul tasto **Sfogliare**, dopodiché nella finestra standard del SO Windows indicare la posizione del file chiave di licenza per **Server** `enterprise.key`.

   Alla prima installazione del **Server** scegliere **Creare un nuovo database** e nel campo **Creare database, utilizzando la chiave data per Dr.Web Enterprise Agent** indicare il file della chiave per software di workstation (`agent.key`).

   Se si vuole conservare il database del **Server** dell'installazione precedente, nel gruppo dei tasti di scelta di database scegliere **utilizzare il database a disposizione**. Si può indicare il file del database di seguito (v. passo **10**).

   Per provare i prodotti si possono utilizzare i file della chiave demo. Premere sul tasto **Chiavi demo** per passare al sito web della società **Doctor Web** ed ottenere i file della chiave demo (v. File della chiave demo).

   Premere sul tasto **Avanti**.

6. Si apre la finestra di scelta del tipo di installazione. Se si sceglie il tipo **Completa**, saranno installati tutti i componenti di **Enterprise Server**, se si sceglie il tipo **Personalizzata**, sul passo successivo si possono impostare i componenti da installare. Dopo la scelta del tipo di installazione premere sul tasto **Avanti**.



Se si programma di utilizzare come database esterno ODBC per Oracle, scegliere la voce **Personalizzata** e nella finestra aperta annullare l'installazione di client incorporato per i DBMS Oracle (nella sezione **Database support - Oracle database driver**).

Nel caso contrario l'operazione con il database non sarà possibile per il conflitto di librerie.

7. Se sul passo precedente è stato scelto il tipo di installazione **Completa**, si apre la finestra di scelta di cartella di installazione. Se si deve modificare la cartella di installazione predefinita, premere sul tasto **Modificare** e scegliere la cartella di installazione. Premere sul tasto **Avanti**.

   Se sul passo precedente è stato indicato il tipo di installazione **Personalizzata**, si apre la finestra di scelta dei componenti installati e delle cartelle per ognuno di essi. Nel menu contestuale dei componenti si può modificare il metodo della loro installazione: installare il componente su computer locale o per avvio in rete (non è disponibile per tutti) o annullare l'installazione del componente. Se si deve modificare la cartella di installazione del componente scelto nella lista, premere sul tasto **Modificare** e indicare la cartella di installazione. Premere sul tasto **Avanti**.

8. Nella finestra successiva si può scegliere la lingua dei moduli di messaggi, impostare la modalità di utilizzo e il nome della risorsa condivisa di sistema per la cartella di installazione di **Agent** (di default si imposta il nome nascosto della risorsa condivisa) e impostare le configurazioni di gestione di file di logging di installazione.

   Se si vuole avviare il **Server** automaticamente dopo l'installazione, mettere il flag **Avviare il servizio nel processo di installazione**.

   Se si vuole aggiungere il **Server** nelle eccezioni di Firewall del sistema operativo (oltre il SO Windows 2000), mettere il flag **Aggiungere alle eccezioni di Firewall le porte e le interfacce del server**.

9. Nella finestra successiva alla prima installazione del **Server**

premere semplicemente sul tasto **Avanti**. Le chiavi di codifica verranno automaticamente generate nel processo di installazione.

Se si installa il **Server** per la rete antivirus esistente, mettere il flag **Utilizzare chiavi di codifica esistenti** e indicare il file con la chiave chiusa, dopodiché verrà creato il file con la chiave aperta (contenuti della chiave aperta corrisponderanno ai contenuti della precedente chiave aperta). Questo permette agli **Agent** di riconoscere il **Server** installato. Nel caso contrario dopo l'installazione si deve copiare la nuova chiave di codifica aperta su tutte le workstation, su cui in precedenza sono stati installati **Enterprise Agent**.

10. Dopo, se sul passo **4** si è scelto il database esistente, appare la finestra di dialogo, in cui si può indicare il file di configurazione del **Server**, preparato in anticipo.

    Nelle finestre di dialogo successive si impostano le configurazioni principali, conservati nel file di configurazione del **Server** (v. Allegato G1. File di configurazione di Dr.Web Enterprise Server).

11. Nella finestra di dialogo, dedicata alla configurazione di database, si configurano i parametri del database utilizzato, che dipendono dalla scelta del tipo di database al passo **4** e dalla presenza del file di configurazione del Server, impostato al passo **9**.

    Alla creazione di un database nuovo o se non è stato impostato il file di configurazione del **Server** (per il database esistente), indicare il driver da utilizzare. Variante **Driver del database IntDB** prescrive di utilizzare gli strumenti incorporati di **Enterprise Server**. Altri varianti prevedono utilizzo del database corrispondente esterna. Le impostazioni dei parametri di DMBS sono descritte in dettagli in allegati (v. Allegato B. Impostazioni necessarie per utilizzare DBMS. Parametri dei driver DBMS).

    Premere sul tasto **Avanti**.

12. Se per creare un nuovo database al passo precedente si è scelto il **Driver del database IntDB**, nella finestra successiva vengono visualizzate le informazioni sulla creazione di un

nuovo database.

Se con utilizzo del database esistente al passo precedente si è impostato il file di configurazione del **Server** o scelto il **Driver del database IntDB**, nella finestra successiva si deve indicare il file del database. Per farlo, premere il tasto **Sfogliare**. Mettere il flag **Avviare il controllo del database interno durante l'installazione** per controllare l'integrità del database nel processo di installazione del **Server**.

Se al passo precedente si è indicata una delle varianti di DBMS esterni, nella finestra successiva si devono indicare i parametri corrispondenti per impostare accesso al database.

13. Dopo, se al passo **4** si è impostata la creazione di un nuovo database o al passo **9** (per il database esistente) non si è impostato il file di configurazione del **Server** dell'installazione precedente, viene visualizzata la finestra di dialogo della configurazione di rete, dove si configura il protocollo di rete per il **Server** (si può di impostare solo un protocollo di rete; altri protocolli possono essere impostati successivamente).

    Nei campi **Interfaccia** e **Porta** impostare i valori corrispondenti per richiamare il **Server**. Di default è impostata l'interfaccia 0.0.0.0, il che significa, che si può accedere al **Server** per tutte le interfacce.

    Di default viene utilizzata la porta 2193, comunque, per compatibilità con il software antivirus delle versioni precedenti, è anche supportata la porta 2371.

    Per limitare accesso locale al **Server**, mettere il flag **Acceso limitato a Dr.Web Enterprise Server.** L'accesso al programma di installazione, ad **Agent** e ad altri **Server** (nel caso della rete antivirus già esistente, costruita con **Enterprise Security Suite**) sarà proibito. Di seguito queste impostazioni si possono modificare via il menu del **Centro gestione Amministrazione**, voce **Configurazione di Dr.Web Enterprise Server**, scheda **Moduli**.

    Mettere il flag **Servizio rilevamento server** per fare che il

**Server** risponda alle richieste broadcast e alle richieste multicast di altri **Server**.

Per configurare le impostazioni di rete predefinite, premere nella parte inferiore della finestra sul tasto **Standard**. Per limitare operazione del Server a sola interfaccia di rete interna – `127.0.0.1` – premere sul tasto **Limitata**. Con queste impostazioni la gestione del **Server** può essere eseguita solo dal **Centro gestione**, avviato sullo stesso computer, e al **Server** può connettersi solo **Agent**, avviato sullo stesso computer. Di seguito, dopo la messa a punto delle impostazioni del **Server**, le impostazioni di rete si possono modificare.

Premere sul tasto **Avanti**.

14. Se al passo **4** si è scelta la creazione di un database nuovo o al passo **9** (per il database esistente) non è stato impostato il file di configurazione del **Server** dell'installazione precedente, nella finestra successiva viene visualizzata la richiesta di invio statistiche di eventi dei virus nella società **Doctor Web**. Per farlo, mettere il flag **Consentire invio statistiche** e compilare i campi corrispondenti. **Server** di statistiche – `stat.drweb.com`, **URL** – `\update`. Si possono riempire i campi **Utente** e **Password** se è necessario identificare le statistiche inviate (si può ottenere il nome utente e la password nel **Supporto tecnico di Doctor Web**). Nel campo **Inviare ogni** inserire l'intervallo di invio di statistiche in minuti. I campi obbligatori sono solamente l'indirizzo del server di statistiche e l'intervallo di invio di statistiche.

    Inoltre in questa finestra nel caso di utilizzo di un server proxy si possono indicare i parametri di esso. Per farlo, mettere il flag **Utilizzare proxy** e inserire l'indirizzo del server proxy (obbligatorio), il nome utente e la password per accedere ad esso.

    Il flag **Utilizzare proxy** sarà disponibile solo se la cartella di installazione del **Server** non contiene i file di configurazione dell'installazione precedente.

15. Se sul passo **4** si è scelta la creazione di un database nuovo, nella finestra successiva impostare la password

dell'amministratore della rete antivirus.



All'impostazione di password dell'amministratore non si possono utilizzare i caratteri di alfabeti nazionali.

Premere sul tasto **Avanti**.

16. Di seguito si consiglia di impostare l'aggiornamento del repositorio durante l'installazione. Per farlo, mettere il flag **Aggiornare repositorio**. Premere sul tasto **Avanti**.
17. Premere sul tasto **Installare.** Le azioni successive del programma di installazione non richiedono l'intervento dell'utente.
18. Dopo il completamento di installazione premere sul tasto **Finito**.



Dopo l'installazione del **Server**, per consentire una corretta generazione di collegamenti quando si creano pacchetti di installazione dell'**Agent**, modificare il parametro **ServerName** nel fine di configurazione `webmin.conf` che si trova nella sottocartella `etc` della cartella di installazione di **Enterprise Server**. Decommentare questo parametro e invece di www.example.com specificare l'indirizzo IP o il nome DNS del computer su cui è installato **Enterprise Server**, e inoltre il numero della porta nel formato:

`ServerName` *<Indirizzo_Server>*`:`*<numero_porta>*

Salvare le modifiche apportate e riavviare **Enterprise Server.**

Se si usa un cluster di **Enterprise Server**, e anche se su **Enterprise Server** si usa una porta personalizzata, modificare i parametri corrispondenti nel file di configurazione `download.conf` che si trova nella sottocartella `etc` della cartella di installazione di **Enterprise Server** (vedi inoltre l'Allegato G3. File di configurazione download.conf).

Di solito, la gestione di **Enterprise Server** installato viene eseguita via il **Centro gestione** di **Dr.Web**. Il programma di installazione mette inoltre nel menu principale del SO Windows gli elementi, che permettono di eseguire la configurazione e la gestione del **Server**.

Nel menu **Start** → **Programmi** viene locata la cartella di **Dr.Web Enterprise Server**, che contiene i seguenti elementi:

- Cartella **Gestione server** contiene i comandi di avvio, riavvio e completamento dell'operazione del **Server**, nonché i comandi della configurazione di logging ed altri comandi del **Server**, descritti in più dettagli in Allegato H5. Dr.Web Enterprise Server.
- Voce **Interfaccia web** per aprire il **Centro gestione** e connettersi al **Server**, installato su questo computer (all'indirizzo http://localhost:9080).
- Voce **Documentazione** – per aprire la documentazione dell'amministratore nel formato HTML.

***Cartella di installazione di Dr.Web Enterprise Server ha la seguente struttura:***

- `bin` – file eseguibili di **Enterprise Server**.
- `etc` – cartella contiene i file delle impostazioni principali dei componenti della rete antivirus, nonché le chiavi di licenza del **Server** (`enterprise.key`) e **Agent** (`agent.key`).
- `Installer` – contiene programma di installazione per installare **Antivirus** su computer protetto e chiave di codifica aperta (`drwcsd.pub`).
- `update-db` – script, necessari per aggiornare la struttura dei database del **Server**.
- `var` – cartella contiene le sottocartelle:
  - `backup` – serve per conservare il backup dei database e di altri dati critici;
  - `extensions` – contiene gli script dell'utente, destinati ad automatizzare l'esecuzione di certi processi, tutti gli script di default sono disattivati;
  - `repository` – cosidetta cartella di aggiornamenti, dove vengono messi aggiornamenti attuali di database dei virus,

di file dei pacchetti antivirus e di componenti della rete antivirus. Cartella contiene sottocartelle per i componenti singoli funzionali del software, e all'interno di essi – sottocartelle per diversi SO. Cartella deve essere disponibile per modifica all'utente, a cui nome viene avviato il **Server** (nei SO della famiglia UNIX questo, di solito, è l'utente **drwcs**, nei SO Windows — **LocalSystem**);

- `templates` – moduli di log.

◆ `webmin` – cartelle contengono gli elementi del **Centro gestione** di **Dr.Web**: documentazione, icone, moduli.



I contenuti della cartella di aggiornamenti `\var \repository` vengono scaricati dal server di aggiornamenti tramite il protocollo HTTP automaticamente, secondo l'orario installato per **Server**; inoltre l'amministratore della rete antivirus può mettere aggiornamenti in queste cartelle manualmente.

## 2.2.2. Installazione di Dr.Web Enterprise Server per i SO della famiglia UNIX®



Tutte le azioni di installazione si devono eseguire dalla console a nome di superutente (**root**).

***Per installare Dr.Web Enterprise Server per i SO della famiglia UNIX:***

1. Per avviare l'installazione del pacchetto `drweb-esuite`, eseguire il seguente comando:

| Per Server con | Comando |
|---|---|
| SO FreeBSD | `pkg_add` *<file_di_distribuzione>*`.tbz` |
| SO Solaris | 1. `bzip2 -d` *<file_di_distribuzione>*`.bz2` |

| Per Server con | | Comando |
|---|---|---|
| | | 2. `pkgadd -d` *<file_di_distribuzione>* |
| SO Linux | Debian®<br>Ubuntu® | `dpkg -i` *<file_di_distribuzione>*`.deb` |
| | pacchetti rpm | `rpm -i` *<file_di_distribuzione>*`.rpm` |



Se è già installato il software di **Enterprise Server**, si può eseguire l'aggiornamento dei componenti installati. Per farlo, avviare la distribuzione, utilizzando il seguente comando:

- per distribuzioni **rpm**:

  `rpm -U` *<nome_file_di_distribuzione>*`.rpm`

- per pacchetti **deb**:

  `dpkg -i` *<nome_file_di_distribuzione>*`.deb`

Inoltre esistono cosidetti pacchetti `generic`, che possono essere installati su qualsiasi sistema operativo della famiglia Linux, compreso quella non inclusa nella lista dei supportati ufficialmente.



Durante l'installazione dei pacchetti `generic` sui SO della famiglia Linux deve essere presente la libreria `glibc` della stessa versione che la versione del pacchetto `generic`.

Installazione viene eseguita con il programma di installazione, inclusa nel pacchetto. Utilizzare il seguente comando:

`tar -xjf` *<nome_file_distribuzione>*`.tar.bz2`

Dopodiché a nome del superutente eseguire lo script:

```
./drweb-esuite-install.sh
```



Installazione del **Server** può essere sospesa in qualsiasi momento, mandando al processo di installazione qualsiasi dei seguenti segnali: `SIGHUP`, `SIGINT`, `SIGTERM`, `SIGQUIT` e `SIGWINCH` (nel sistema operativo **FreeBSD** la modifica delle dimensioni della finestra del terminal comporta la spedizione del segnale `SIGWINCH`). Alla sospensione del processo di installazione viene eseguito il ripristino completo dei cambiamenti nel file system al punto prima di installazione. Installazione del pacchetto rpm può essere interrotta, premendo i tasti CTRL + C.

Premere il tasto ESC nel processo di installazione del **Server** permette di tornare al passo precedente di installazione. In questo caso, al passo 2 (prima finestra del programma di installazione con l'accordo di licenza) il tasto ESC interrompe il funzionamento del programma di installazione.

Nome dell'amministratore della rete antivirus predefinito **admin**.

2. Nelle finestre successive (numero e conseguenza della loro apparenza dipende dalla famiglia del SO) vengono visualizzati i messaggi di diritti d'autore e il testo dell'Accordo di licenza. Per continuare l'installazione si deve accettare l'accordo di licenza.
3. Di seguito si propone di impostare il gruppo e l'utente, a cui nome opererà **Server**. Stesso utente sarà il proprietario dei file di **Enterprise Server**.

   Alla richiesta di creazione utente scegliere la voce **nuovo** per creare un utente nuovo, a cui nome viene inviato il complesso. Nel menu successivo si consiglia di lasciare il valore predefinito e premere su **OK**. Nel menu della scelta del gruppo creare un nuovo gruppo. Nella richiesta successiva lasciare il valore predefinito.

4. Di seguito si propone di indicare i percorsi ai file chiavi del **Server** (`enterprise.key`) e **Agent** (`agent.key`), che vengono forniti insieme alla distribuzione, e, se si aggiorna dalla versione precedente, sono salvati di default in `/root/esuite_backup` o nella cartella indicata.



Durante l'installazione nella modalità di console il numero dei tentativi di impostazione delle chiavi (se indicate scorrettamente) è limitato:

- per i SO FreeBSD - 3 tentativi;
- per i SO Solaris - 2 tentativi.

All'impostazione non corretta delle chiavi, alla scadenza del numero tentativi ammissibile, l'operazione del programma di installazione viene sospesa.

5. Di seguito:
   - Nel caso di installazione del software nei SO **Solaris**: si propone di creare un nuovo database del Server. Se si esegue l'aggiornamento del **Server**, e si dispone di un database salvato, inserire no, premere su ENTER e indicare il percorso al file salvato con database.
     Se è, invece, la prima installazione di **Enterprise Server** premere su ENTER e indicare la password dell'amministratore (utente **admin**), che avrà accesso al **Server**. Si può lasciare la password predefinita - **root**. All'impostazione di una password, per le ragioni di sicurezza, la password inserita non viene visualizzata sullo schermo in nessun modo. Si deve inserire la password due volte (nel caso password inserite siano diverse, si deve rifare la procedura – seguire le istruzioni che appaiono). Password deve contenere non meno di 4 caratteri.
     Di seguito si propone di creare le chiavi di codifica nuove. Se si dispone delle chiavi salvate `drwcsd.pri` e `drwcsd.pub`, rifiutare a crearne nuove (digitare no, premere su ENTER) e indicare il percorso completo ai file esistenti. Se non ce ne sono le chiavi, premere su ENTER per creare le nuove chiavi di codifica.

- Nel caso di installazione via pacchetti **deb**: si propone di inserire la password dell'amministratore (utente **admin**). Si può lasciare la password predefinita - **root**. All'impostazione di una password, per le ragioni di sicurezza, la password inserita non viene visualizzata sullo schermo in nessun modo. Si deve inserire la password due volte (nel caso password inserite siano diverse, si deve rifare la procedura – seguire le istruzioni che appaiono). Password deve contenere non meno di 4 caratteri.
- In altri casi: si propone di inserire la password dell'amministratore (utente **admin**). All'impostazione di una password, per le ragioni di sicurezza, la password inserita non viene visualizzata sullo schermo in nessun modo. Si deve inserire la password due volte (nel caso password inserite siano diverse, si deve rifare la procedura – seguire le istruzioni che appaiono). Password deve contenere non meno di 8 caratteri.



Nell'impostazione della password dell'amministratore non è ammissibile utilizzo di caratteri di alfabeti nazionali.

All'aggiornamento e all'avvio del database manuali la password dell'amministratore viene ripristinata al valore predefinito.

Per rispettare le politiche di sicurezza si consiglia di non lasciare i dati di registrazione predefiniti. I dati di registrazione (nome utente e password) sono richiesti alla connessione al **Server** via il **Centro gestione**.

6. Se è presente l'interprete perl, nonostante il SO utilizzato, può essere proposto di eseguire la configurazione di alcuni parametri del **Server**. A richiesta di configurazione dei certi tipi di parametri la variante no è predefinita (sul tasto ENTER), il che significa, che per tali parametri saranno impostati i valori predefiniti. Alla scelta `yes` viene proposto di indicare i valori dei parametri proposti (in questo caso i valori dei parametri predefiniti saranno indicati nelle parentesi quadre, per impostarli basterà premere il tasto ENTER).

   La procedura di configurazione dei parametri del **Server** si può iniziarla manualmente (per farlo è inoltre necessario che sia

installato l'interprete perl). Per farlo, è sufficiente avviare lo script `configure.pl`, che si trova in:

- nella cartella `/usr/local/drwcs/bin/` per i SO **FreeBSD**,
- nella cartella `/opt/drwcs/bin/` per i SO **Linux** e il SO **Solaris**.

Parametri di utilizzo dello script `configure.pl` sono riportati in allegato H5.9. Configurazione di Dr.Web Enterprise Server per i SO della famiglia UNIX.

7. Di seguito viene eseguita l'installazione del software, durante la quale il programma di installazione può richiedere la conferma delle proprie azioni a nome dell'amministratore.



Dopo l'installazione del **Server**, per consentire una corretta generazione di collegamenti quando si creano pacchetti di installazione dell'**Agent**, modificare il parametro **ServerName** nel file di configurazione `webmin.conf` che si trova nella cartella:

- `/var/drwcs/etc` per SO **FreeBSD** e per SO **Solaris**
- `/var/opt/drwcs/etc` per SO **Linux**

Decommentare questo parametro e invece di www.example.com specificare l'indirizzo IP o il nome DNS del computer su cui è installato **Enterprise Server**, e inoltre il numero della porta nel formato:

`ServerName` *<DNS_nome>*`:`*<numero_porta>*

Salvare le modifiche apportate e riavviare **Enterprise Server**.

Se si usa un cluster di **Enterprise Server**, e anche se su **Enterprise Server** si usa una porta personalizzata, modificare i parametri corrispondenti nel file di configurazione `download.conf`, che si trova nella cartella:

- `/var/drwcs/etc` per SO **FreeBSD** e per SO **Solaris**
- `/var/opt/drwcs/etc` per SO **Linux**

(vedi inoltre l'Allegato G3. File di configurazione download.conf).



Nel processo di installazione del software nei SO **FreeBSD** viene creato lo script `rc`:

`/usr/local/etc/rc.d/drwcsd.sh`.

Utilizzare i comandi:

- `/usr/local/etc/rc.d/drwcsd.sh stop` - per arresto manuale del **Server**;
- `/usr/local/etc/rc.d/drwcsd.sh start` - per avvio manuale del **Server**.

Nel processo di installazione del software nei SO **Linux** e **Solaris** viene creato lo script `init` per avvio e arresto del **Server**: `/etc/init.d/drwcsd`, che utilizza `/opt/drwcs/bin/drwcs.sh`. L'ultimo non è destinato all'avvio manuale.

## 2.2.3. Installazione del plugin Dr.Web Browser-Plugin



L'installazione del plugin **Dr.Web Browser-Plugin** per i browser Mozilla Firefox, Opera e Chrome è possibile solo per le versioni che funzionano sotto i SO Windows e i SO della famiglia Linux.

Il plugin **Dr.Web Browser-Plugin** è necessario per il lavoro completo con il **Centro gestione** (v. anche Requisiti di sistema per il Centro gestione Dr.Web).

Il plugin viene fornito insieme alla distribuzione del **Server** e può essere installato:

1. Automaticamente, a richiesta del browser web nel processo di operazione con il **Centro gestione**, in particolare con gli elementi che richiedono di caricare il plugin (per **Scanner di rete**, all'installazione remota dei componenti antivirus).

2. Manualmente, via l'installazione del plugin **Dr.Web Browser-Plugin**.

## *Installazione manuale di Dr.Web Browser-Plugin*

***Per scaricare il programma di installazione del plugin Dr.Web Browser-Plugin per l'installazione manuale:***

1. Aprire il **Centro gestione**. Se **Dr.Web Browser-Plugin** non è ancora installato per il browser web utilizzato, sotto il menu principale viene visualizzato il consiglio di installare il plugin.
2. Seguire il link **Installare Dr.Web Browser-Plugin**.


Dr.WEB
Browser-Plugin
Dr.Web Browser-Plugin consente di usare le piene funzionalità del Pannello di Controllo Dr.Web Enterprise suite. Dr.Web Browser-Plugin include lo scanner di porte e il modulo di aggiornamento dei componenti antivirus su remoto.
Dr.Web Browser-Plugin per Firefox 12 (x86)
Scarica
Versione a 64 bit di Dr.Web Browser-Plugin
© 2012 Doctor Web
Politica di riservatezza

**Immagine 2-4. Sezione per scaricare plugin Dr.Web Browser-Plugin**

3. Nella sezione scarico del plugin è riportata la versione del browser web attuale e i bit presumibili (x86 o x64) del plugin.

   Per i SO della famiglia UNIX si propone inoltre di scegliere dalla lista a cascata la versione della distribuzione per il SO corrispondente.

4. Per scaricare e salvare il plugin premere sul tasto **Scaricare**. Dopodiché si può installarlo manualmente.
5. Per passare a un'altra versione di bit, premere sul link sotto il tasto dello scarico, dopodiché si può scaricare il programma di installazione come descritto nel passo **4**.

### *Per installare il plugin Dr.Web Browser-Plugin nei SO Windows:*

1. Inviare il file della distribuzione. Si apre la finestra di **InstallShield Wizard**, che avvisa sul prodotto installato. Premere sul tasto **Avanti**.
2. Si apre la finestra con il testo di accordo di licenza. Dopo aver letto i termini dell'accordo di licenza nel gruppo di tasti di scelta indicare **Accetto i termini dell'accordo di licenza** e premere sul tasto **Avanti**.
3. Se apre la finestra di scelta della cartella di installazione. Se è necessario modificare la cartella di installazione predefinita, premere sul tasto **Modificare** e scegliere la cartella di installazione. Premere sul tasto **Avanti**.
4. Nella seguente finestra premere sul tasto **Installare** per iniziare il processo di installazione. Le azioni successive del programma di installazione non richiedono l'intervento dell'utente.
5. Dopo il completamento dell'installazione premere sul tasto **Finito**.

### *Per installazione del plugin Dr.Web Browser-Plugin nei SO della famiglia UNIX:*

Eseguire il seguente comando:

- per i pacchetti **deb**:
  `dpkg -i drweb-esuite-plugins-linux-`<*versione_distribuzione*>`.deb`
- per i pacchetti **rpm**:
  `rpm -i drweb-esuite-plugins-linux-`<*versione_distribuzione*>`.rpm`
- per altri sistemi (pacchetti **tar.bz2** e **tar.gz**):
  1. Decomprimere l'archivio con il plugin.
  2. Creare la cartella per i plugin, se non è ancora creata.

  Per esempio, per il browser Mozilla Firefox: `mkdir /usr/lib/mozilla/plugins`

3. Copiare nella cartella per i plugin la libreria, decompressa al passo 1.

Per esempio, per il browser Mozilla Firefox: `cp libnp*.so /usr/lib/mozilla/plugins`



Dopo l'installazione del plugin **Dr.Web Browser-Plugin** sotto il SO della famiglia UNIX, riavviare il browser web se era avviato.

# 2.3. Installazione di Dr.Web Enterprise Agent per SO Windows®



Installazione di **Enterprise Agent** deve essere eseguita dall'utente con i diritti dell'amministratore di tale computer.

Se su workstation è già installato **Agent**, prima di iniziare un'installazione nuova si deve eliminare **Agent** installato.

***Installazione di Enterprise Agent e del pacchetto antivirus può essere eseguita in due modi:***

1. In remoto: su **Enterprise Server** via LAN. Viene eseguita dall'amministratore della rete antivirus. In questo caso è richiesto l'intervento dell'utente. Per le descrizioni più dettagliate v. sezione Installazione remota di Dr.Web Enterprise Agent per SO Windows®.
2. Localmente: direttamente su workstation dell'utente. Può essere eseguita sia dall'amministratore, sia dall'utente. In questo caso per l'installazione si può utilizzare (v. inoltre File di installazione):
   - Pacchetto di installazione `esinst.exe`.
   - Installazione di rete di **Agent** `drwinst`.

***Durante l'installazione di Enterprise Agent su server LAN e su computer del cluster si deve considerare:***

- Nel caso di installazione su computer, che eseguono il ruolo dei terminal server (nel SO Windows sono installati i servizi **Terminal Services**), per fornire il lavoro di **Agent** alle terminal sessioni l'installazione di Agent deve essere eseguita solo localmente via l'installazione guidata e eliminazione dei programmi sul **Pannello di controllo** del SO Windows.
- Su server, che hanno funzionalità importanti di rete (controller di dominio, server di distribuzione licenze ecc), si sconsiglia di installare i componenti **SpIDer Gate**, **SpIDer Mail** e **Dr.Web Firewall** per evitare eventuali conflitti dei servizi di rete e dei componenti interni dell'antivirus **Dr.Web**.
- Installazione di **Agent** su cluster deve essere eseguita separatamente per ogni nodo del cluster.
- I principi del funzionamento di **Agent** e dei componenti del pacchetto antivirus su nodo cluster sono analoghi a quelli su server standard di LAN, quindi si sconsiglia di installare su nodi del cluster i componenti **Dr.Web Firewall**, **SpIDer Mail**, **SpIDer Gate**.
- Se l'accesso alle risorse quorum del cluster è strettamente limitato, si consiglia di escluderlo dal controllo della guardia **SpIDer Guard** e limitarsi con controlli regolari della risorsa con lo **Scanner**, avviato nel modo programmato o manualmente.

## 2.3.1. File di installazione

### *Pacchetto di installazione (esinst)*

Alla creazione di una nuova utenza viene generato un pacchetto di installazione `esinst` per installazione di **Agent**.

Il link per scaricare il pacchetto di installazione di **Agent** per una singola workstation è disponibile:

1. Appena creata una nuova workstation (v. passo **11** nella sezione Creazione di una nuova utenza).

2. Dopo la creazione di workstation sempre:
   - nella sezione proprietà di workstation,
   - nella sezione **Oggetti scelti** quando si sceglie una workstation nella lista gerarchica.

## *Installazione di rete (drwinst)*

Installazione di rete di **Agent** `drwinst`, nonché la chiave di codifica aperta `drwcsd.pub` si trovano nella cartella `Installer` (di default risorsa condivisa nascosta) della cartella di installazione di **Enterprise Server**. Disponibilità di risorsa in rete viene impostata nel passo 8 all'installazione di **Enterprise Server**. Di seguito si può modificare questa risorsa a sua scelta.

Inoltre installazione per installare **Agent** e chiave di codifica aperta sono disponibili sulla pagina di installazione del **Centro gestione Dr.Web**.

## *Pagina di installazione*

Nella pagina di installazione del **Centro gestione Dr.Web** si possono scaricare:

1. Installazione di rete di **Agent** `drwinst`.

   Installazioni per i vari SO si trovano nelle cartelle con i nome corrispondenti.

2. Chiave di codifica aperta `drwcsd.pub`.

Pagina di installazione è disponibile su qualsiasi computer, che ha accesso di rete a **Enterprise Server**, all'indirizzo:

`http://`*<indirizzo_server>*`:`*<numero_porta>*`/install/`

dove come *<indirizzo_server>* indicare indirizzo IP o nome DNS del computer, su cui è installato **Enterprise Server**. Come *<numero_porta>* indicare porta numero `9080` (o `9081` per https).

## 2.3.2. Installazione di Dr.Web Enterprise Agent con il pacchetto di installazione

***Per installare Agent con pacchetto di installazione è necessario:***

1. Con il **Centro gestione**:
   - Creare utenza di nuovo utente sul **Server**.
   - Ottenere il link per scaricare il programma di installazione di **Agent**.
2. Inviare all'utente il link al programma di installazione di **Agent**.
3. Eseguire l'installazione di Agent su workstation. Di solito l'installazione del software di **Enterprise Agent** viene eseguita dall'utente stesso.
4. Autorizzazione di una nuova workstation antivirus sul **Server** di default viene eseguita automaticamente (v. anche Politica connessione workstation nuove).

### 2.3.2.1. Creazione di una nuova utenza

Per creare un'utenza o più utenze nuove, utilizzare il Centro gestione di Dr.Web.



Assicurarsi, che per il parametro **ServerName** nel file di configurazione `webmin.conf` è stato impostato il valore:

*<Indirizzo_Server>*`:9080`,

dove *<Indirizzo_Server>* - indirizzo IP o nome DNS del computer, su cui è installato **Enterprise Server**.



Alla creazione di utenza è necessario che la connessione del **Centro gestione** al **Server** venga eseguita all'indirizzo IP per il dominio, su cui viene creata l'utenza. Nel caso contrario all'installazione del pacchetto non sarà possibile collegarsi al **Server**, siccome alla creazione del pacchetto di installazione di **Enterprise Agent**, in esso viene definito l'indirizzo del **Server,** a cui è connesso il **Centro gestione**.

Alla connessione del **Centro gestione** al **Server** da una workstation locale controllare che l'indirizzo del **Server** non sia impostato come loopback (`127.0.0.1`).

***Per creare un nuovo utente via il Centro gestione di Dr.Web:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**.
2. Nella barra degli strumenti premere sul tasto  **Aggiungere workstation o gruppo**. Nel sottomenu aperto scegliere la voce  **Creare workstation**. Nella parte destra della finestra del **Centro gestione** si apre il pannello di creazione di utenza.
3. Nel campo **Numero** indicare il numero utenti da creare.
4. Nel campo **Identificatore** viene automaticamente generato identificatore unico di workstation creata. Se necessario, si può sostituirlo.
5. Nel campo **Nome** impostare il nome workstation, che viene visualizzato nella lista gerarchica della rete antivirus. Di seguito, dopo la connessione di workstation al **Server**, questo nome può essere automaticamente sostituito con il nome workstation, impostato localmente.
6. Nei campi **Password** e **Ripetere password** indicare la password per accesso di workstation al **Server**.



Alla creazione di più utenze i campi **Identificatore**, **Nome** e **Password** (**Ripetere password**) saranno impostate automaticamente e non saranno disponibili alla modifica alla fase di creazione di workstation.

7. Nel campo **Descrizione** inserire l'informazione supplementare

su utente. Questo parametro non è obbligatorio.

8. Nella sezione **Gruppo** scegliere i gruppi, di cui farà parte la workstation antivirus creata. Di default la workstation fa parte del gruppo **Everyone**. Se esistono gruppi utenti, ci si può includere la workstation creata. Per farlo, premere sul nome gruppo nella sezione **Gruppi conosciuti**. Per escludere workstation da gruppi utente, di cui fa parte, premere sul nome gruppo nella sezione **Appartenenza a**.

   Per impostare il gruppo primario per una workstation creata, premere sull'icona del gruppo richiesto nella sezione **Appartenenza a**. In questo caso sull'icona del gruppo appare **1**.

   Non si può escludere la workstation dal gruppo **Everyone** e dal gruppo primario.

9. Se necessario, compilare la sezione **Sicurezza**. La descrizione delle impostazioni di questa sezione è riportata in Configurazione di workstation.
10. Se necessario, compilare la sezione **Location**.
11. Premere **Salvare** nell'angolo destro superiore. Si apre la finestra di creazione con successo di una workstation nuova, dove sarà indicato il numero di identificazione e il link per scaricare la distribuzione di **Agent**.



Link per scaricare il programma di installazione di **Agent** è inoltre disponibile:

- nelle proprietà di workstation dopo la sua creazione,
- nella sezione **Oggetti scelti** durante la scelta di workstation creata nella lista gerarchica.

V. anche File di installazione.

12. Le azioni per l'installazione del software dell'**Agent** sono descritte sotto.



Installazione di **Enterprise Agent** deve essere eseguita da utente con i diritti dell'amministratore dello stesso computer.

Se su workstation è già installato il software antivirus, prima di iniziare l'installazione, il programma di installazione farà il tentativo di eliminarlo. Se il tentativo fallisce, l'utente dovrà per contro proprio eliminare il software antivirus, utilizzato su workstation.

### 2.3.2.2. Installazione di Dr.Web Enterprise Agent e del pacchetto antivirus

***Per installazione di Dr.Web Enterprise Agent e del pacchetto antivirus su workstation:***

1. Scaricare il file di installazione di **Agent**. Per farlo, passare per link, ottenuto alla creazione di workstation nel Centro gestione.
2. Avviare su workstation il file scaricato `esinst.exe`. Si apre la finestra di installazione guidata di **Dr.Web** Anti-virus.
3. Prima di iniziare l'installazione guidata chiede di confermare che non ci siano installati i programmi antivirus. Assicurarsi che sul computer non si utilizza altro software (compreso il software di altre versioni dei programmi antivirus di **Dr.Web**), dopodiché mettere il flag **Sul computer non ce ne sono altri antivirus**. Premere sul tasto **Avanti**.
4. Nella finestra successiva si propone la scelta delle varianti di installazione:
   - **Rapida (consigliata)** - la variante di installazione più semplice. Tutti i parametri vengono impostati automaticamente. Dopo passare al passo **8**.
   - **Personalizzata** - variante di installazione, in cui l'utente può scegliere i componenti del software antivirus, installato sul computer.
   - **Amministrativa** - la variante più completa di installazione. Permette di impostare/modificare tutti i parametri di installazione e del software installato.
5. Per varianti di installazione **Personalizzata** e **Amministrativa**: nella finestra successiva si propone di scegliere i componenti del pacchetto antivirus **Dr.Web**. Mettere i flag accanto ai componenti da installare sul computer.

Nella sezione **Percorso alla cartella di installazione** si può impostare la cartella, in cui viene installato il software antivirus. Di default è la cartella di `Dr.Web Enterprise Suite`, locato nella cartella `Program files` sul disco di sistema. Per impostare/modificare il percorso predefinito, premere sul tasto **Sfogliare** e indicare il percorso richiesto.

Premere sul tasto **Avanti**.

Dopodiché per la variante di installazione **Personalizzata** passare al passo **8**.

6. Per variante di installazione **Amministrativa**: nella finestra successiva impostare le configurazioni di **Installazione di rete**:
   - Nel campo **Dr.Web Enterprise Server** viene impostato indirizzo di rete di **Enterprise Server**, da cui viene eseguita l'installazione di **Agent** e del pacchetto antivirus. Se all'avvio di installazione si imposta l'indirizzo del **Server,** viene automaticamente aggiunto in questo campo.



All'installazione di **Enterprise Agent** con installazione, creata nel **Centro gestione,** viene automaticamente compilato il campo **Dr.Web Enterprise Server**.

Se non si conosce l'indirizzo del **Server**, premere sul tasto **Ricerca**. Viene visualizzata la finestra per cercare **Enterprise Server** attivi di rete. Impostare i parametri necessari (nel formato *<nome_server>*`@`*<indirizzo_IP>*`/`*<prefisso_rete>*`:`*<porta>*) e premere sul tasto **Ricerca**. Nella lista dei **Server** rilevati scegliere quello, da cui viene installato il software antivirus, e premere sul tasto **OK**.

   - Nel campo **Dr.Web Enterprise Server chiave pubblica** viene impostato il percorso completo alla chiave di codifica aperta (`drwcsd.pub`), locata sul computer dell'utente (all'avvio di installazione dal **Server** per la rete, la chiave viene copiata nei file temporanei del SO, dopodiché viene messa nella cartella di installazione).

- Nella sezione **Utilizzare compressione allo scarico** scegliere la variante necessaria di compressione del traffico: **Sì** - utilizzare compressione, **No** - non utilizzare, **Possibile** - utilizzo di compressione del traffico dipende dalle impostazioni sul **Server**.
- Flag **Aggiungere Dr.Web Agent nella lista delle esclusioni di Windows Firewall** prescrive di aggiungere le porte e le interfacce, utilizzate da **Agent**, alla lista delle esclusioni di Firewall del sistema operativo. Si consiglia di mettere questo flag. Questo permette di evitare gli errori, per esempio, all'aggiornamento automatico dei componenti di antivirus e dei database dei virus.
- Se necessario, mettere il flag **Registrare agent nella lista dei programmi installati**.

Quest'opzione consente, fra le altre funzioni, di eliminare l'**Agent** e il pacchetto antivirus con gli strumenti regolari del SO Windows (vedi la voce Rimozione dei componenti di software per SO Windows®).

7. Per la variante di installazione **Amministrativa**: nella finestra successiva impostare le configurazioni di **Agent**:
   - Nella sezione **Autorizzazione** sono impostati i parametri di autorizzazione di Agent sul Server. Alla scelta di variante **Automaticamente (predefiniti)** i parametri di autorizzazione (identificatore e password) verranno automaticamente generate sul **Server**, in questo caso la modalità di accesso di workstation verrà definita sul **Server** (v. Politica connessione workstation). Alla scelta della variante **Manuale** si devono impostare i parametri di autorizzazione workstation: il suo **Identificatore** sul **Server** e la **Password** di accesso ad esso. In questo caso workstation riceve l'accesso senza la conferma manuale dell'Amministratore sul **Server**.



All'installazione di **Enterprise Agent** con l'installazione, creata nel **Centro gestione**, vengono automaticamente compilati i campi **Identificatore** e **Password** per la variante di autorizzazione **Manuale**.

- Nelle sezioni **Compressione** e **Codifica** vengono impostate le seguenti modalità per il traffico tra **Server** e Agent (per più informazioni v. Utilizzo codifica e compressione del traffico).

Premere su **Avanti**.

8. Inizia l'installazione di **Agent** e dei componenti antivirus (non richiede l'intervento di utente).
9. Dopo il completamento di installazione il wizard di installazione avvisa di necessità di riavviare il computer. Premere sul tasto **Finito** per completare l'operazione di Installazione guidata.
10. Riavviare il computer.



Subito dopo l'installazione sul computer **Agent** automaticamente stabiliscono la connessione al **Server**. Appena **Agent** stabilisce la connessione al **Server**, nella finestra del **Centro gestione** appare il nome della workstation corrispondente.

**Enterprise Agent** può essere installato su workstation in remoto, utilizzando il **Centro gestione**.

## 2.3.3. Installazione di Dr.Web Enterprise Agent con Installazione di rete



Prima della prima installazione di **Enterprise Agent** si deve obbligatoriamente aggiornare il repositorio del **Server** (v. Aggiornamento manuale dei componenti di Dr.Web Enterprise Security Suite, v. **Verifica disponibilità aggiornamenti**).

Se l'installazione di rete è avviata nella modalità di installazione standard (cioè senza la chiave `-uninstall`) su una workstation, dove è già stata eseguita l'installazione, non comporta esecuzione di qualche azione. L'installazione completa il suo funzionamento e visualizza la finestra con la lista delle chiavi ammissibili.

***Installazione con Installazione di rete è disponibile in due modalità principali:***

1. Nella modalità background.
2. Nella modalità grafica.

Si può installare **Enterprise Agent** su workstation in remoto, utilizzando il **Centro gestione** o utilizzando le funzionalità del servizio **Active Directory** (v. Installazione remota di Dr.Web Enterprise Agent).

### 2.3.3.1. Installazione di Dr.Web Enterprise Agent nella modalità background di installazione

***Per installare Dr.Web Enterprise Agent su workstation nella modalità background di installazione:***

1. Dal computer, su cui viene installato software antivirus, entrare nella cartella di rete di installazione di **Agent** (all'installazione del **Server** è la sottocartella `Installer` della cartella di installazione del **Server**, di seguito si può spostarlo) e avviare il programma `drwinst`.

   Di default il comando `drwinst`, avviato senza parametri, utilizza la modalità **Multicast** per la scansione di rete per la presenza di **Enterprise Server** attivi e esegue il tentativo di installazione di **Agent** dal primo **Server**, rilevato in rete.

   Se si utilizza la modalità **Multicast** per la ricerca dei **Server** attivi, l'installazione di **Agent** viene eseguita dal primo **Server** rilevato. In questo caso se la chiave `pub` in possesso non corrisponde alla chiave del **Server**, l'installazione viene completata con errore. In questo caso indicare esplicitamente l'indirizzo del **Server** all'avvio di installazione (v. sotto).

   Inoltre il comando `drwinst` può essere avviato con i parametri supplementari:

- Nel caso in cui la modalità **Multicast** non viene utilizzata, all'installazione di **Agent** si consiglia di utilizzare il nome del **Server** (in precedenza registrato nel servizio DNS):

```
drwinst <nome_DNS_del_Server>
```

Questo semplifica il processo di configurazione di rete antivirus, legato alla procedura di reinstallazione di **Enterprise Server** su altro computer.

- Si può inoltre utilizzare indicazione esplicita dell'indirizzo del **Server**, per esempio:

```
drwinst 192.168.1.3
```

- Utilizzo della chiave `-regagent` permette all'installazione di **Agent** di registrarlo nella lista di installazione e di disinstallazione dei programmi.
- Per avviare l'installazione nella modalità grafica utilizzare il parametro `-interactive`.



La lista completa dei parametri di **Installazione di rete** è riportata in Allegato H4. Installazione di rete.

2. Dopo il completamento del funzionamento dell'installazione sul computer viene installato il software di **Agent** (ma non il pacchetto antivirus).
3. Dopo la conferma di workstation al **Server** (se richiesto dalle impostazioni del **Server**) il pacchetto antivirus viene installato automaticamente.
4. Riavviare il computer a richiesta dell'**Agent**.

### 2.3.3.2. Installazione di Dr.Web Enterprise Agent nella modalità grafica di installazione

***Per installare Dr.Web Enterprise Agent su workstation nella modalità grafica di installazione:***

1. Dal computer, su cui viene installato il software antivirus, entrare nella cartella di rete di installazione di **Agent** (all'installazione del Server è la sottocartella `Installer` della cartella di installazione del Server, di seguito si può spostarlo) e avviare il programma `drwinst` con il parametro `-interactive`.

   Si apre la finestra di installazione guidata di **Dr.Web** Anti-virus.

2. Prima di iniziare l'installazione, l'installazione guidata chiede di confermare, che sul computer non sono installati programmi antivirus. Assicurarsi che sul computer non venga utilizzato altro software antivirus (compreso software di altre versioni dei programmi antivirus di **Dr.Web**), dopodiché mettere il flag **Sul computer non ce ne sono altri antitivirus**. Premere sul tasto **Avanti**.
3. Nella finestra successiva viene proposta la scelta della variante di installazione:
   - **Rapida (consigliata)** - la variante di installazione più semplice. Tutti i parametri sono impostati automaticamente. Dopo passare al passo **7**.
   - **Personalizzata** - variante di installazione, in cui l'utente può scegliere tutti i componenti del software antivirus, installato sul computer.
   - **Amministrativa** - la variante più completa di installazione. Permette di impostare/modificare tutti i parametri di installazione e del software antivirus installato.
4. Per le varianti di installazione **Personalizzata** e **Amministrativa**: nella finestra successiva si propone la scelta dei componenti del pacchetto antivirus **Dr.Web**. Mettere i flag accanto ai componenti da installare sul computer.

   Nella sezione **Percorso alla cartella di installazione** si può

impostare la cartella dove viene installato il software antivirus. Di default è la cartella `Dr.Web Enterprise Suite`, locata nella cartella `Program files` sul disco di sistema. Per impostare / modificare il percorso predefinito, premere sul tasto **Sfogliare** e indicare il percorso richiesto.

Premere sul tasto **Avanti**.

Dopo per la variante di installazione **Personalizzata** passare al passo **7**.

5. Per la variante di installazione **Amministrativa**: nella finestra successiva impostare le configurazioni di **Installazione di rete**:
   - Nel campo **Dr.Web Enterprise Server** viene impostato l'indirizzo di rete di **Enterprise Server**, da cui viene eseguita l'installazione di **Agent** e del pacchetto antivirus. Se all'avvio di installazione si imposta l'indirizzo del **Server,** viene automaticamente compilato in questo campo. Se non si sa l'indirizzo del **Server**, premere sul tasto **Ricerca**. Viene visualizzata la finestra per la ricerca di **Enterprise Server** attivi di rete. Impostare i parametri necessari (nel formato *<nome_server>*`@`*<indirizzo-IP>*`/`*<prefisso_rete>*`:`*<porta>*) e premere sul tasto **Ricerca**. Nella lista dei **Server** rilevati scegliere quello, da cui viene installato il software antivirus, e premere sul tasto **OK**.
   - Nel campo **Dr.Web Enterprise Server chiave pubblica** viene impostato il percorso completo alla chiave aperta di codifica (`drwcsd.pub`), locata sul computer dell'utente (all'avvio di installazione dal **Server** per la rete, la chiave viene copiata nei file temporanei del SO, dopodiché viene spostata nella cartella di installazione).
   - Nella sezione **Utilizzare compressione allo scarico** scegliere la variante richiesta di compressione del traffico: **Sì** – utilizzare le compressione, **No** – non utilizzare, **Possibile** – utilizzo della compressione del traffico dipende dalle impostazioni sul **Server**.

- Flag **Aggiungere Dr.Web Agent nella lista delle esclusioni di Windows Firewall** prescrive di aggiungere le porte e le interfacce, utilizzate da **Agent**, alla lista delle esclusioni di Firewall del SO. Si consiglia di mettere questo flag. Questo permette di evitare errori, per esempio, all'aggiornamento automatico dei componenti di antivirus e dei database dei virus.
- Se necessario, mettere il flag **Registrare Agent nella lista di programmi installati**.

Quest'opzione consente, fra le altre funzioni, di eliminare l'**Agent** e il pacchetto antivirus con gli strumenti regolari del SO Windows (vedi la voce Rimozione dei componenti di software per SO Windows®).

6. Per la variante di installazione **Amministrativa**: nella finestra successiva impostare le configurazioni dell'**Agent**:
   - Nella sezione **Autorizzazione** si impostano i parametri di autorizzazione di **Agent** sul **Server**. Se si sceglie la variante **Automaticamente (predefinita)** i parametri di autorizzazione (identificatore e password) verranno automaticamente generate sul **Server**, e in questo caso la modalità di accesso di workstation sarà definita sul **Server** (v. Politica connessione workstation). Alla scelta di modalità **Manuale** si devono impostare i parametri di autorizzazione di workstation: il suo **Identificatore** sul **Server** e la **Password** di accesso ad esso. In questo caso la workstation ottiene accesso senza la conferma manuale dell'amministratore sul **Server**.
   - Nelle sezioni **Compressione** e **Codifica** si impostano le modalità corrispondenti per il traffico tra il **Server** e **Agent** (per più informazioni v. Utilizzo di codifica e di compressione traffico).

   Premere su **Avanti**.
7. Comincia l'installazione di **Enterprise Agent**. Dopo l'installazione di **Agent** premere sul tasto **Finito** per completare il funzionamento dell'Installazione guidata.
8. Dopo la conferma di workstation sul **Server** (se richiesto dalle impostazioni del **Server**, v. Politica connessione workstation e se sul passo **6** all'**Installazione amministrativa** non è stata scelta la variante di autorizzazione **Manuale**), il pacchetto

antivirus viene installato automaticamente.

9. Riavviare il computer a richiesta dell'**Agent**.

## 2.4. Installazione remota di Dr.Web Enterprise Agent per i SO Windows®

**Dr.Web Enterprise Security Suite** permette di rilevare i computer, su cui non è ancora installata la protezione antivirus **Dr.Web Enterprise Security Suite**, e in alcuni casi di installare tale protezione in remoto.



Installazione remota di **Enterprise Agent** è disponibile solo per le workstation, che operano sotto la gestione del SO della famiglia Windows 2000 e superiori (vedi Allegato A. Lista completa delle versioni dei SO supportate), escluse le edizioni Starter e Home.

Installazione remota di **Enterprise Agent** è possibile solo tramite il **Centro gestione** avviato nei sistemi operativi Windows XP o superiore (vedi Allegato A. Lista completa delle versioni dei SO supportate), escluse le edizioni Starter e Home.

Per installare in remoto **Enterprise Agent** su workstation si devono avere i diritti dell'amministratore delle workstation corrispondenti.

Installazione remota non richiede la configurazione supplementare di workstation remota, se fa parte del dominio e viene utilizzata l'utenza dell'amministratore del dominio. Nel caso se la workstation remota non fa parte del dominio o si utilizza utenza locale per l'installazione, per una serie delle versioni dei SO Windows è necessaria la configurazione supplementare della workstation remota.

## *Configurazione supplementare all'installazione remota su workstation fuori dominio o con utilizzo di utenza locale*



Le impostazioni indicate possono diminuire la sicurezza della workstation remota. Si consiglia di venire a conoscenza della destinazione di configurazioni indicate prima di apportare le modifiche nel sistema o annullare l'installazione remota e installare **Agent** manualmente.

All'installazione remota di **Agent** su workstation esterna al dominio e/o con utilizzo di utenza locale, sul computer, su cui verrà installato **Agent**, si devono eseguire le seguenti azioni:

| SO | Configurazione |
|---|---|
| ◆ Windows 2000<br>◆ Windows Server 2000 | Configurazione supplementare non è richiesta. |
| ◆ Windows XP | **1.** Impostare modalità accesso ai file condivisi: **Pannello di controllo** → **Opzioni cartella** → Scheda **Visualizzazione** → togliere il flag **Utilizza condivisione file semplice (scelta consigliata).**<br>**2.** Impostare nelle politiche locali la modalità seguente del modello di autenticazione di rete: **Pannello di controllo** → **Strumenti di amministrazione** → **Politica locale di sicurezza** → **Parametri di sicurezza** → **Politiche locali** → **Parametri di sicurezza** → **Accesso di rete: modello di condivisione e di sicurezza per utenze locali** → **Standard – utenti locali sono autorizzati come stessi**. |

| SO | Configurazione |
|---|---|
| ◆ Windows Server 2003 | Configurazione supplementare non è richiesta. |
| ◆ Windows Vista<br>◆ Windows 7<br>◆ Windows Server 2008 | 1. Attivare opzione **Accesso condiviso ai file**: **Pannello di controllo** → **Rete e internet** → **Centro connessioni di rete e condivisione** → **Condivisione e individuazione** → **Condivisione file** → **Attivare**.<br>2. Attivare l'utenza incorporata dell'amministratore e impostare la sua password. Durante l'installazione utilizzare questa utenza: **Pannello di controllo** → **Sistema e manutenzione** → **Strumenti di amministrazione** → **Gestione computer** → **Utenti e gruppi locali** → **Utenti**. Fare il click con il tasto sinistro sulla voce **Amministratore** → togliere il flag **Bloccare utenza** → **OK**. Cliccare con il tasto destro sulla voce → **Impostare password** → impostare password. |

Se l'utenza sulla workstation remota ha la password vuota, impostare nelle politiche locali la politica di accesso con la password vuota: **Pannello di controllo** → **Strumenti di amministrazione** → **Politica di sicurezza locale** → **Opzioni di sicurezza** → **Politiche locali** → **Opzioni di sicurezza** → **Utenza: disattivare utilizzo di password vuote solamente per accesso console** → **Disattivare**.



Si devono locare il file di installazione di **Agent** `drwinst.exe` e la chiave aperta di codifica `drwcsd.pub` sulla risorsa condivisa.

## 2.4.1. Installazione di Dr.Web Enterprise Agent con il Centro gestione di Dr.Web

***Sono possibili i seguenti modi dell'installazione remota di Agent su workstation della rete:***

1. Installazione tramite Scanner di rete.

   Consente di cercare prima dell'installazione i computer della rete che non sono protetti e di installare su di essi **Enterprise Agent**.

2. Installazione tramite Installazione per la rete.

   Si consiglia di usare questo metodo se si conosce in anticipo l'indirizzo della workstation o del gruppo di workstation sulle quali vengono installati gli **Agent**.

3. Installazione su workstation con ID impostati.

   Consente di installare su workstation o gruppi di workstation **Agent** per gli account selezionati (anche per tutti gli account nuovi) per cui sono stati impostati ID e password di accesso al **Server**.



Per una corretta operatività dello **Scanner di rete** e dello strumento **Installazione per la rete** nel browser Windows Internet Explorer, l'indirizzo IP e/o il nome DNS del computer, su cui è installato **Enterprise Server**, devono essere inseriti tra i siti attendibili del browser, in cui si usa il **Centro gestione** per l'installazione remota.

## Utilizzo dello Scanner di rete

Nella lista gerarchica della rete antivirus del **Centro gestione** vengono visualizzati i computer, già inclusi nella composizione di rete. **Dr.Web Enterprise Security Suite** inoltre permette di rilevare i computer, non protetti dal software antivirus di **Dr.Web ESS** e di installare i componenti antivirus in remoto.

Per eseguire velocemente l'installazione del software di **Agent** su workstation, si consiglia di utilizzare **Scanner di rete** (v. Scanner di rete), che esegue la ricerca dei computer per indirizzi IP.

### *Per installare Agent, utilizzando Scanner di rete:*

1. Aprire Scanner di rete. Per farlo, scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione Scanner di rete. Si apre la finestra con lo stesso nome senza i dati caricati.
2. Indicare nel campo di input di **Reti** la lista dei reti nel formato:
   - separati da un trattino (per esempio, `10.4.0.1-10.4.0.10`),
   - separati da una virgola e uno spazio (per esempio, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
   - utilizzando il prefisso di rete (per esempio, `10.4.0.0/24`).

   La descrizione dettagliata delle impostazioni aggiuntive è riportata nella sezione Scanner di rete.
3. Premere sul tasto **Avvia lo scanner**. Nella finestra viene caricato il catalogo (la lista gerarchica) dei computer con indicazione, sui quali il software antivirus è installato e sui quali no.
4. Esplorare gli elementi del catalogo, corrispondenti ai gruppi di lavoro (domini). Tutti gli elementi di catalogo, corrispondenti ai gruppi di lavoro e a workstation singoli sono marcati con icone diverse, il cui valore è riportato sotto.

**Tabella 2-1. Vari tipi di icone**

| Icona | Descrizione |
|---|---|
| **Gruppi di lavoro** | |
|  | Gruppi di lavoro, che oltre ad altri comprendono i computer, su cui si può installare **Dr.Web ESS**. |
|  | Altri gruppi, che comprendono i computer con il software antivirus installato o non disponibili per la rete. |

| Icona | Descrizione |
|---|---|
| | **Workstation** |
| | Workstation rilevata è annoverata nel database ed è attiva (workstation attive con il software antivirus installato). |
| | Workstation rilevata è annoverata nel database nella tabella di workstation eliminate. |
| | Workstation rilevata non è annoverata nel database (sulla workstation non c'è il software antivirus). |
| | Workstation rilevata non è annoverata nel database (workstation è connessa ad altro **Server**). |
| | Workstation rilevata è annoverata nel database, non è attiva e la porta è chiusa. |

Elementi del catalogo, corrispondenti alle workstation con le icone o , si possono inoltre esplorare e prendere conosenza di composizione dei componenti installati.

Quando si preme sull'icona di componenti di workstation, connessa a tale **Server**, viene visualizzata la finestra delle impostazioni di tale componente.

5. Nella finestra di **Scanner di rete** scegliere il computer non protetto (oppure più computer non protetti utilizzando i tasti CTRL o SHIFT).
6. Scegliere nella barra degli strumenti la voce **Installa Dr.Web Enterprise Agent**.
7. Si apre la finestra di creazione del compito di installazione di **Agent.**
8. Nella sezione **Dr.Web Network Installer** si possono impostare le configurazioni di installazione del software di **Agent**.
9. Nel campo **I Computer** viene indicato l'indirizzo IP del computer (dei computer), su cui viene installato il software antivirus.
   - Se il software viene installato sui computer trovati mediante lo **Scanner di rete,** nel campo **Computer** sarà già indicato l'indirizzo della workstation o di più workstation sulle quali verrà eseguita l'installazione.

- Nel caso contrario, impostare l'indirizzo del computer o di più computer. All'installazione del software di **Agent** contemporaneamente su più computer si possono indicare più indirizzi IP dei computer nel seguente formato:
  - separati da un trattino (per esempio, `10.4.0.1-10.4.0.10`),
  - con virgola e spazio (per esempio, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
  - con utilizzo del prefisso di rete (per esempio, `10.4.0.0/24`).



Inoltre invece di indirizzi IP si possono indicare i nomi di dominio dei computer.

Se per l'installazione viene usato un nome del computer che contiene un trattino '-', questo nome deve essere racchiuso tra virgolette, per esempio "123-456".

10. Di default il software dell'**Agent** viene installato nella cartella `C:\Program Files\DrWeb Enterprise Suite`. Se necessario, indicare altro percorso nel campo **Cartella d'installazione**.
11. Di default nel campo **Server** viene visualizzato l'indirizzo IP o il nome DNS di **Enterprise Server**, al cui è connesso il **Centro gestione**. Se necessario, indicare in questo campo l'indirizzo del **Server**, da cui viene installato il software antivirus.
12. Nel campo **Chiave aperta** viene indicato il percorso alla chiave aperta, nel campo **File eseguibile** – nome completo di installazione di rete. Se necessario, correggere valori impostati e impostare altri parametri necessari.



I percorsi alla chiave aperta o ai file eseguibili devono essere indicati nel formato di indirizzi di rete.

13. Se necessario, inserire nel campo **Parametri aggiuntivi** i parametri della riga di comando di installazione di rete (per più informazioni v. Allegato H4. Installazione di rete).
14. Nella lista a cascata **Dettagli del log** impostare il livello di

dettagli nella gestione del protocollo di installazione.

15. Nel campo **Time-out dell'installazione (secondi)** impostare il tempo massimo di attesa del completamento di installazione di **Agent** in secondi. Valori ammissibili: 1-600. Di default è impostato il valore di 180 secondi. Con capacità bassa del canale di comunicazione tra **Server** e **Agent** si consiglia di aumentare il valore di tale parametro.
16. Se necessario, mettere il flag **Registra l'installazione nella base di dati dei programmi installati**.
17. Nella sezione **Installa** scegliere i componenti del pacchetto antivirus, che vengono installati su workstation. Inoltre impostare i parametri di compressione del traffico all'installazione.
18. Nella sezione **Autorizzazione** indicare i parametri di autorizzazione per accesso al computer remoto.

    Si possono impostare più utenze dell'amministratore. Per farlo:

    a) Premere sul tasto  , per aggiungere account, indicata nella sezione **Autorizzazione** account nella lista di account, utilizzati durante l'installazione.

    b) Per aggungere un'altra utenza, di nuovo riempire i campi con le impostazioni dell'autorizzazione e premere sul tasto  . Fare lo stesso per ciascun account nuovo.

    c) Nella lista di utenze utilizzate si possono escludere o consentire di utilizzare le utenze disattivate in precedenza. Per farlo, togliere da o mettere il flag su account corrispondenti.

    All'installazione di **Agent** prima si utilizza la prima utenza dalla lista. Se l'installazione sotto questa utenza viene completata con errore, si utilizza l'utenza successiva ecc.

19. Dopo l'impostazione dei parametri necessari di sezione **Dr.Web Network Installer**, premere su **Avanti**.
20. Nella scheda di **Dr.Web Enterprise Agent per Windows** si possono indicare parametri come:

- Nella sezione **Autorizzazione** si possono indicare i parametri di autorizzazione di **Agent** sul **Server**. Se il flag **Impostare parametri** non è attivato e non sono riempiti i campi corrispondenti, i parametri di autorizzazione saranno impostati automaticamente.
- Nelle sezioni **Codifica** e **Compressione** si può consentire utilizzo di codifica e di compressione del traffico tra **Agent** e **Server**.

Di seguito questi parametri si possono modificare nelle impostazioni di Enterprise Agent e nelle proprietà di workstation.

21. Dopo aver inserito tutti i parametri necessari premere su **Installa**.



Per avviare l'installazione del software antivirus si utilizza il servizio incorporato.

22. **Enterprise Agent** viene installato su workstation indicate. Dopo la conferma di workstation sul **Server** (se lo richiedono le impostazioni di **Enterprise Server**, v. anche Creazione di rete antivirus semplice), viene automaticamente installato il pacchetto antivirus.
23. Riavviare il computer a richiesta dell'**Agent**.

## Utilizzo dello strumento Installazione per la rete

Quando la base di rete antivirus è già creata e si deve installare il software dell'**Agent** su certi computer, si consiglia di utilizzare l'**Installazione per la rete**.

***Per installazione per la rete:***

1. Scegliere la voce **Amministrazione** del menu principale, nella finestra aperta scegliere la voce del menu di gestione **Installazione per la rete**.
2. Passi successivi di installazione sono uguali ai passi **8-23** sopra.

## Installazione per account con ID impostati

***Per installare Agent in remoto per account con ID selezionati:***

a) Se si crea un nuovo account della workstation:

1. Creare un nuovo account o più nuovi account delle workstation (vedi la voce Creazione di nuovo account).
2. Subito dopo la creazione del nuovo account, nella parte destra della finestra principale si apre un pannello con l'intestazione **Installa Dr.Web Agent**. Premere sul tasto **OK**.
3. Si apre la finestra dello **Scanner di rete**.
4. Passi successivi di installazione sono uguali ai passi **2-23** della procedura descritta sopra.
5. Completata l'installazione, controllare se nella lista gerarchica sono cambiate le icone delle workstation corrispondenti.

b) Se si utilizza un account già esistente della workstation:

1. Nella lista gerarchica della rete antivirus selezionare una nuova workstation, un gruppo di workstation, su cui non sono ancora stati installati gli **Agent**, oppure il gruppo **New** (per installare su tutti i nuovi account disponibili).
2. Sul pannello degli strumenti premere **Installa Dr.Web Enterprise Agent**.
3. Si apre la finestra dello **Scanner di rete**.
4. Passi successivi di installazione sono uguali ai passi **2-23** della procedura descritta sopra.
5. Completata l'installazione, controllare se nella lista gerarchica sono cambiate le icone delle workstation corrispondenti.

L'installazione dell'**Agent** su workstation con ID selezionati è accessibile anche per l'amministratore di gruppi.



Se ci sono errori durante l'installazione remota, rivolgersi alla sezione Diagnostica dei problemi di installazione remota.

## 2.4.2. Installazione di Dr.Web Enterprise Agent con il servizio Active Directory

Se nella rete locale protetta si utilizza il servizio **Active Directory**, si può installare **Enterprise Agent** su workstation in remoto.



Installazione di **Agent** con il servizio Active Directory è inoltre disponibile con il File System Distribuito DFS (v. sezione Utilizzo di DFS all'installazione di Agent via Active Directory).

### Installazione di Agent

***Per installare Agent, utilizzando il servizio Active Directory:***

1. Scaricare dal sito http://download.drweb.com/esuite/ il programma di installazione di **Enterprise Agent** per le reti con **Active Directory**.
2. Sul server della rete locale, che supporta il servizio **Active Directory**, eseguire l'installazione amministrativa di **Enterprise Agent**. L'installazione può essere eseguita sia nella modalità a riga di comando **(A)**, sia nella modalità grafica del programma di installazione **(B)**.



All'aggiornamento del **Server** non è necessario aggiornare il programma di installazione di **Enterprise Agent** per le reti con Active Directory. Dopo l'aggiornamento del software del **Server**, **Agent** e software antivirus su workstation vengono aggiornati automaticamente dopo l'installazione.

## *(A) Configurazione di parametri di installazione di Dr.Web Enterprise Agent nella modalità a riga di comando*

avviare il seguente comando con tutti i parametri necessari e con il parametro obbligatorio di disattivazione della modalità grafica `/qn`:

`msiexec /a` *<nome_pacchetto>*`.msi /qn [`*<parametri>*`]`

Chiave `/a` avvia la decompressione del pacchetto amministrativo.

**Nome pacchetto**

Nome del pacchetto di installazione di **Enterprise Agent** per le reti con **Active Directory** di seguito è rappresentato nel seguente formato:

`drweb-es-agent-`*<versione>*`-`*<data-release>*`-windows-nt-`*<numero_bit>*`.msi`.

**Parametri**

`/qn` - parametro di disattivazione della modalità grafica. All'utilizzo di questa chiave si devono impostare i seguenti parametri obbligatori:

- `ESSERVERADDRESS=`*<nome_DNS>* - indica l'indirizzo di **Enterprise Server**, al cui viene connesso **Agent.** Per formati possibili v. Allegato E3.
- `ESSERVERPATH=`*<percorso_nome_file>* - indica il percorso completo alla chiave aperta di codifica di **Enterprise Server** e al nome del file (di default il file `drwcsd.pub` nella sottocartella `Installer` della cartella di installazione di **Enterprise Server**).

- `TARGETDIR` - cartella di rete per l'immagine di **Agent** (il pacchetto di installazione di **Agent** modificato), che viene scelta via editor delle politiche dei gruppi per l'installazione impostata. Tale cartella deve essere disponibile per la lettura e la scrittura. Il percorso alla cartella si deve indicare nel formato di indirizzi di rete, anche se è disponibile localmente; la cartella deve essere obbligatoriamente disponibile dalle workstation destinate.



Prima dell'installazione amministrativa la cartella di destinazione per l'immagine di **Agent** (v. parametro `TARGETDIR`) non deve contenere il programma di installazione di **Enterprise Agent** per le reti con **Active Directory** (*<nome_pacchetto>*`.msi`).



Dopo la decompressione del pacchetto amministrativo nella cartella:

*<cartella_di_destinazione>*`\Program Files\DrWeb Enterprise Suite`

ci deve essere solamente il file `README.txt`.

**Esempi:**

```
msiexec /a ES_Agent.msi /qn
ESSERVERADDRESS=servername.net ESSERVERPATH=\
\win_serv\drwcs_inst\drwcsd.pub TARGETDIR=\\comp
\share
```

```
msiexec /a ES_Agent.msi /qn
ESSERVERADDRESS=192.168.14.1
ESSERVERPATH="C:\Program Files\DrWeb Enterprise
Server\Installer\drwcsd.pub" TARGETDIR=\\comp
\share
```

Stessi parametri si possono impostare nella modalità grafica di installazione.

Dopodiché sul server della rete locale, dove è installato il software di gestione di **Active Directory**, si deve programmare l'installazione del

pacchetto (v. procedura sotto).

## *(B) Configurazione dei parametri di installazione di Dr.Web Enterprise Agent nella modalità grafica*



Prima dell'installazione amministrativa assicurarsi che la cartella di destinazione dell'immagine di **Agent** non contiene il programma di installazione di **Enterprise Agent** per le reti con **Active Directory** (*<nome_pacchetto>*`.msi`).



Dopo la decompressione del pacchetto amministrativo nella cartella:

*<cartella_di_destinazione>*`\Program Files\DrWeb Enterprise Suite`

ci deve essere solamente il file `README.txt`.

1. Per avviare il programma di installazione nella modalità grafica eseguire il comando:

   `msiexec /a` *<percorso_al_programma_installazione>* `\`*<nome_pacchetto>*`.msi`

2. Si apre la finestra **InstallShield Wizard**, che ci avvisa sul prodotto installato. Premere sul tasto **Avanti**.



L'installazione di **Agent** utilizza la lingua, impostata nelle configurazioni di lingua del computer.

3. Nella finestra nuova indicare il nome DNS o l'indirizzo IP di **Enterprise Server** (v. Allegato E3). Indicare la posizione della chiave aperta di **Enterprise Server** (`drwcsd.pub`). Premere sul tasto **Avanti**.
4. Nella finestra successiva indicare la cartella di rete, dove viene scritto l'immagine di **Agent**. Si deve indicare il percorso all'immagine nel formato di indirizzi di rete, anche se la cartella è disponibile localemente; la cartella deve obbligatoriamente essere disponibile dalle workstation di destinazione. Premere

sul tasto **Installare**.

5. Dopo il completamento dell'installazione viene automaticamente richiamata la finestra di configurazione, con cui si può programmare l'installazione di pacchetti sui computer di rete.

## *Configurazione di installazione di pacchetto su workstation scelte*

1. Nel **Pannello di controllo** (o nel menu **Start** per i SO Windows 2003/2008 Server, nel menu **Start** → **Programmi** per il SO Windows 2000 Server) scegliere **Strumenti di amministrazione** → **Active Directory – utenti e computer** (nella modalità grafica di installazione di **Agent** il richiamo di questa finestra delle impostazioni viene eseguito automaticamente).
2. Nel dominio, che include i computer, su cui si prevede l'installazione di **Enterprise Agent**, creare una nuova **Unità** (per il SO Windows 2000 Server - **Unità organizzativa**) con il nome, per esempio, **ESS**. Per farlo, nel menu contestuale del dominio scegliere **Creare** → **Unità**. Nella finestra aperta inserire il nome di una nuova unità e premere su **OK**. Includere nell'unità creata i computer, su si prevede di installare **Agent**.
3. Aprire la finestra di modifica di politiche di gruppi. Per farlo:
   a) per il SO Windows 2000/2003 Server: nel menu contestuale dell'unità creata **ESS** scegliere la voce **Proprietà**. Nella finestra aperta di proprietà passare alla scheda **Politiche di gruppo**.
   b) per il SO Windows 2008 Server: premere su **Start** → **Strumenti di amministrazione** → **Gestione di politica di gruppo**.
4. Per l'unità creata impostare la politica di gruppo. Per farlo:
   a) nel SO Windows 2000/2003 Server: premere sul tasto **Aggiungere** e creare l'elemento della lista con il nome di politica **ESS**. Fare il doppio click su di esso.

b) nel SO Windows 2008 Server: nel menu contestuale dell'unità creata **ESS** scegliere la voce **Creare un nuovo oggetto nel dominio e legarlo**. Nella finestra aperta impostare il nome di nuovo oggetto della politica di gruppo e premere sul tasto **OK.** Nel menu contestuale della politica di gruppo nuova scegliere la voce **Modificare**.

5. Nella finestra aperta **Editor di gestione di politiche di gruppo** inserire le configurazioni per la politica di gruppo, creata nella v. **4**. Per farlo:
   a) nel SO Windows 2000/2003 Server: nella lista gerarchica scegliere l'elemento **Configurazione computer** → **Configurazione programmi** → **Installazione programmi**.
   b) nel SO Windows 2008 Server: nella lista gerarchica scegliere l'elemento **Configurazione computer** → **Politiche** → **Configurazione programmi** → **Installazione programmi**.
6. Nel menu contestuale dell'elemento **Installazione programmi** scegliere la voce **Creare** → **Pacchetto**.
7. Di seguito impostare il pacchetto di installazione di **Agent**. Per farlo, indicare l'indirizzo della risorsa di rete condivisa (l'immagine di **Agent**, creata alla sua installazione amministrativa). Il percorso alla cartella con il pacchetto si deve indicare nel formato di indirizzi di rete, anche se la cartella è disponibile localmente.
8. Si apre la finestra **Decompressione dei programmi**. Scegliere l'opzione **Programmati**. Premere su **OK**.
9. Nella finestra di editor di gestione di politiche di gruppo appare la voce **Dr.Web Enterprise Agent**. Nel menu contestuale di questa voce scegliere **Proprietà**.
10. Nella finestra aperta di proprietà del pacchetto passare alla scheda **Decompressione**. Premere sul tasto **Avanzate**.
11. Si apre la finestra **Parametri avanzati decompressione**.
    - Mettere il flag **Non utilizzare le impostazioni di lingua alla decompressione**.

- Se si programma di installare **Enterprise Agent** tramite pacchetto msi configurabile sui sistemi operativi a 64 bit, mettere il flag **Rendere quest'applicazione a 32 bit accessibile per computer a x64 bit**.

12. Fare il doppio click su **OK**.
13. **Enterprise Agent** sarà installato su computer scelti alla loro registrazione successiva nel dominio.

## Applicazione delle politiche con considerazione delle configurazioni precedenti di Agent

Alla impostazione di politiche di Active Directory per l'installazione di **Agent**, si deve considerare la possibilità di presenza di **Agent** già installato su workstation. Sono possibili tre varianti:

1. **Su workstation non c'è Enterprise Agent**.

   Dopo l'applicazione di politiche, **Agent** viene installato a secondo delle regole generali.

2. **Su workstation è già installato Enterprise Agent senza il servizio Active Directory**.

   Dopo l'applicazione della politica di Active Directory, **Agent** installato rimane su workstation.



In questo caso **Agent** su workstation è installato, ma per il servizio Active Directory **Agent** è considerato non installato. Quindi dopo ogni avvio di workstation viene ripetuto il tentativo fallito di installare **Agent** via il servizio Active Directory.

   Per l'installazione di **Agent** via Active Directory si deve manualmente (o con il **Centro gestione**) eliminare l'**Agent** installato e di nuovo impostare le politiche di Active Directory per tale workstation.

3. **Su workstation è già installato Enterprise Agent con il servizio Active Directory**.

Dopo l'applicazione della politica:

a) Se per la workstation sono consentiti i diritti di eliminazione di **Agent**, viene eliminato da workstation. Per l'installazione di **Agent** via Active Directory si devono di nuovo impostare le politiche di Active Directory per tale workstation.



In questo caso si devono di nuovo impostare le politiche per installare **Agent**, siccome, dopo la prima impostazione di politiche, **Agent** di workstation viene eliminato, ma per il servizio Active Directory **Agent** è considerato installato.

b) Se workstation non ha diritti per l'eliminazione di **Agent**, l'impostazione di politiche non comporta i cambiamenti dello stato del software antivirus su workstation. Per le azioni successive si devono impostare i diritti di eliminazione di **Agent** (v. Configurazione diritti utente) e si devono di nuovo impostare le politiche di Active Directory per tale workstation. Dopodiché le azioni sono uguali alla v. **a)**.



L'impostazione di politiche di Active Directory di nuovo può essere eseguita in qualsiasi modo comodo.

# 2.5. Installazione di NAP Validator

**Dr.Web NAP Validator** serve per controllare l'operabilità del software antivirus delle workstation protette.

Questo componente si installa sul computer con il server NAP configurato.

***Per installare NAP Validator eseguire le seguenti azioni:***

1. Avviare il file di distribuzione. Si apre la finestra di scelta di lingua, in cui si eseguirà l'installazione del prodotto successiva. Sceglire l'**italiano** e premere sul tasto **Avanti**.

2. Si apre la finestra **InstallShield Wizard**, che avvisa sull'installaizone del prodotto. Premere sul tasto **Avanti**.
3. Si apre la finestra con il testo di accordo di licenza. Dopo aver letto i termini dell'accordo di licenza nel gruppo di tasti di scelta indicare **Accetto i termini dell'accordo di licenza** e premere sul tasto **Avanti**.
4. Nella finestra aperta nei campi **Indirizzo** e **Porta** impostare rispettivamente l'indirizzo IP e la porta di **Enterprise Server**. Premere sul tasto **Avanti**.
5. Premere sul tasto **Installare**. Le azioni successive del programma di installazione non richiedono l'intervento dell'utente.
6. Dopo il completamento di installazione premere sul tasto **Finito**.

Dopo l'installazione di **Dr.Web NAP Validator** si deve aggiungere **Enterprise Server** al gruppo dei server NAP affidati. Per farlo:

1. Aprire il componente di configurazione del server NAP (comando `nps.msc`).
2. Nella sezione **Gruppi dei server di correzione** premere sul tasto **Aggiungere**.
3. Nella finestra aperta di dialogo indicare il nome del server di correzione e l'indirizzo IP di **Enterprise Server**.
4. Per salvare le modifiche apportate cliccare sul tasto **OK**.

# 2.6. Installazione di Server proxy

Uno o più **Server proxy** possono far parte della rete antivirus.

Scegliendo il computer, su cui viene installato il **Server proxy**, utilizzare come criterio principale il fatto che il **Server proxy** deve essere disponibile da tutte le reti/tutti i segmenti di reti, tra cui esso reindirizza informazione.



Installazione del **Server proxy** deve essere eseguita dall'utente con i diritti dell'amministratore di tale computer.

Di seguito viene descritta l'installazione del **Server proxy**. I contenuti e la conseguenza dei passi possono essere diversi a seconda della versione di distribuzione.

***Per installazione del Server proxy sul computer con il SO Windows:***

1. Avviare il file di distribuzione. Si apre la finestra **InstallShield Wizard**, che ci avvisa sull'installazione del prodotto. Premere sul tasto **Avanti**.
2. Si apre la finestra con il testo di Accordo di licenza. Dopo aver letti i termini dell'Accordo di licenza, scegliere nella parte inferiore della finestra la voce **Accetto i termini dell'Accordo di licenza** e premere sul tasto **Avanti**.
3. Si apre la finestra di scelta della cartella di installazione. Se si deve modificare la cartella di installazione predefinita, premere sul tasto **Modificare** e scegliere la cartella di installazione. Premere sul tasto **Avanti**.
4. Si apre la finestra di configurazione dei parametri del **Server proxy**:
   - Nel campo **Ascoltare** impostare l'indirizzo IP, che ascolta il **Server proxy**. Predefinito - `any (0.0.0.0)` – "ascoltare" tutte le interfacce.
   - Nel campo **Porta** impostare il numero di porta che ascolterà il **Server proxy**. La porta predefinita è la porta **2193** o la porta **23** per il protocollo NetBIOS.
   - Nella lista a cascata **Protocollo** scegliere il tipo di protocollo per ricevere le connessioni in entrata con il **Server proxy**.
   - Mettere il flag **Attivare rilevamento** per attivare la modalià di imitazione del **Server**. Tale modalità permette a **Scanner di rete** di rilevare il **Server proxy** come **Enterprise Server**.

- Nel campo **Gruppo multicast** impostare l'indirizzo IP del gruppo multicast, di cui fa parte **Server proxy**. L'interfaccia indicata viene ascoltata dal **Server proxy** per interazione con **Installazione di rete** nella ricerca di **Enterprise Server** di rete attivi. Se il campo si lascia vuoto, il **Server proxy** non fa parte di nessun gruppo multicast.
- Nella sezione **Reindirizzare a** impostare l'indirizzo o la lista di indirizzi dei **Enterprise Server**, su uno di cui vengono reindirizzate le connessioni, stabilite dal **Server proxy**.

Dopo aver configurato le impostazioni del **Server proxy**, premere su **Avanti**.

5. Si apre la finestra che avvisa su disponibilità di installazione del **Server proxy**. Premere sul tasto **Installare**.
6. Dopo il completamento del processo di installazione premere sul tasto **Finito.**

Al completamento dell'installazione si possono modificare i parametri di operazione del **Server proxy**. Per farlo, utilizzare il file di configurazione `drwcsd-proxy.xml`, locato nella cartella di installazione del **Server proxy**. Le impostazioni del file di configurazione sono riportati in Allegato G4.

### *Per installazione del Server proxy sul computer con SO della famiglia UNIX:*

Eseguire il seguente comando:

- per SO **FreeBSD**:
  `pkg_add` *<nome_file_distribuzione>*`.tbz`
- per SO **Solaris**:
  `bzip2 -d` *<nome_file_distribuzione>*`.bz2` e dopo:
  `pkgadd -d` *<nome_file_distribuzione>*
- per SO **Linux**:
  - per SO **Debian** e SO **Ubuntu**:
    `dpkg -i` *<nome_file_distribuzione>*`.deb`

- per **distribuzioni rpm**:
  `rpm -i <nome_file_distribuzione>.rpm`

Esisitono anche i cosidetti pacchetti `generic`, che possono essere installati su qualsiasi sistema operativo della famiglia Linux, compresi quelli non supportati ufficialmente. Eseguire il seguente comando:
`tar -xjf <nome_file_distribuzione>.tar.bz2`

Per farlo, si devono spostare tutti i contenuti dell'archivio decompresso nella cartella radice.



Nel processo di installazione del software nei SO **FreeBSD** viene creato lo script `rc /usr/local/etc/rc.d/0.dwcp-proxy.sh`.

Utilizzare i comandi:

- `/usr/local/etc/rc.d/0.dwcp-proxy.sh stop` - per arresto manuale del **Proxy server**;
- `/usr/local/etc/rc.d/0.dwcp-proxy.sh start` - per avvio manuale del **Proxy server**.

Nel processo di installazione del software nei SO **Linux** e SO **Solaris** viene creato lo scrip `init` per avvio e arresto del **Proxy server** `/etc/init.d/dwcp-proxy`.

# 2.7. Eliminazione dei componenti singoli di Dr.Web Enterprise Security Suite

## 2.7.1. Eliminazione dei componenti del software per i SO Windows®

### Eliminazione di Dr.Web Enterprise Server

Per eliminare il software di **Enterprise Server** o il plugin **Dr.Web Browser-Plugin** avviare il pacchetto di installazione corrispondente al prodotto della versione installata. Il programma di installazione definisce automaticamente il prodotto software e propone di eliminarlo. Per eliminare il software premere sul tasto **Eliminare**.

L'eliminazione del software di **Enterprise Server**, del plugin **Dr.Web Browser-Plugin** può essere eseguita dagli strumenti standard del SO Windows con elemento del **Pannello di controllo** → **Programmi**.

### Eliminazione di Dr.Web Enterprise Agent e del pacchetto antivirus per rete



L'installazione remota e desinstallazione del software di **Agent** sono possibili solamente nella rete locale e richiedono le autorizzazioni dell'amministratore di tale rete.



Se l'eliminazione di **Agent** e del pacchetto antivirus viene eseguita con il **Centro gestione**, la **Quarantena** non verrà eliminato da workstation.

***Per eliminare il software di workstation antivirus in remoto (solo per i SO della famiglia Windows):***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**.
2. Nella finestra aperta nella cartella della rete antivirus scegliere il gruppo richiesto o workstation antivirus singole.
3. Nella barra degli strumenti della cartella della rete antivirus premere su **Generali** → **Desinstalla Dr.Web Enterprise Agent**.
4. Il software di **Agent** e il pacchetto antivirus verranno eliminate da workstation scelte.



Se il comando di avvio di processo di eliminazione viene impostato al momento quando non c'è la connessione tra **Enterprise Server** e workstation antivirus, l'eliminazione del software di **Agent** su workstation antivirus scelta avviene quando tale connessione è ripristinata.

## Eliminazione locale di Dr.Web Enterprise Agent e del pacchetto antivirus



Per poter eliminare **Agent** e il pacchetto antivirus localmente, tale opzione deve essere consentita sul **Server** nella sezione **Diritti**.

Eliminazione del software antivirus di workstation (**Agent** e pacchetto antivirus) può essere eseguito in due modi:

1. Utilizzando gli strumenti standard del SO Windows.
2. Con il programma di installazione di **Agent**.

Se l'eliminazione di **Agent** e del pacchetto antivirus viene eseguita con gli strumenti standard del SO Windows o con il programma di installazione di **Agent**, all'utente viene visualizzata la richiesta di eliminare la **Quarantena**.

## *Eliminazione con gli strumenti standard del SO Windows*

Questo metodo di eliminazione è disponibile solo se durante l'installazione di **Agent** con il programma di installazione grafica è stato messo il flag **Registrare agent nella lista dei programmi installati**.

Se **Agent** è stato installato nella modalità background del programma di installazione, l'eliminazione del software antivirus con gli strumenti standard sarà disponibile solo se durante l'installazione è stata utilizzata la chiave `-regagent`.

Per eliminare **Agent** e il pacchetto antivirus con gli strumenti standard del SO Windows utilizzare l'elemento **Pannello di controllo** → **Programmi** (per istruzioni dettagliate v. **Manuale dell'utente** per **Agent**).

## *Eliminazione con il programma di installazione*

Per eliminare il software di **Agent** e il pacchetto antivirus su workstation localmente, si deve eseguire nella cartella di installazione di **Enterprise Agent** (di default – `C:\Program Files\DrWeb Enterprise Suite`) il comando `drwinst` con il parametro `-uninstall` (o con i parametri `-uninstall -interactive`, se si deve provvedere al controllo del processo di eliminazione).

Per esempio:

```
drwinst -uninstall -interactive
```

## 2.7.2. Eliminazione di Dr.Web Enterprise Agent con il servizio Active Directory

1. Nel pannello di controllo del SO Windows scegliere nel menu **Amministrazione** l'elemento **Active Directory** - **utenti e computer**.
2. Nel dominio scegliere l'Unità organizzativa creata di **ESS**. Nel menu contestuale scegliere la voce **Propietà**. Si apre la finestra **Propietà di ESS**.
3. Passare alla scheda **Politica di gruppi**. Scegliere l'elemento della lista con il nome **Politiche di ESS**. Fare il doppio click su esso. Si apre la finestra **Editor oggetti di politica di gruppi**.
4. Nella lista gerarchica scegliere **Configurazione computer** → **Configurazione programmi** → **Installazione programmi** → **Pacchetto**. Di seguito nel menu contestuale del pacchetto con la distribuzione di **Agent** scegliere **Tutti i processi** → **Eliminare** → **OK**.
5. Nella scheda **Politica di gruppi** premere su **OK**.
6. **Enterprise Agent** verrà eliminato dai computer alla registrazione successiva sul dominio.

## 2.7.3. Eliminazione di Dr.Web Enterprise Server per i SO della famiglia UNIX®



Tutte le azioni di eliminazione si devono eseguire dal nome del super utente (**root**).

***Per eliminare Dr.Web Enterprise Server:***

1. Eseguire il seguente comando:

| Per Server in | Comando |
|---|---|
| SO FreeBSD | `pkg_delete drweb-esuite` |

| Per Server in | | Comando |
|---|---|---|
| SO Solaris | | 1. Arrestare il **Server**: `/etc/init.d/drwcsd stop`<br>2. Eseguire il comando: `pkgrm DWEBesuite` |
| SO Linux | Debian<br>Ubuntu | `dpkg -r drweb-esuite` |
| | pacchetto rpm | `rpm -e drweb-esuite` |
| | pacchetto generic | `/opt/drwcs/bin/drweb-esuite-uninstall.sh` |

Eliminazione del **Server** può essere arrestata in qualsiasi momento, inviando al processo uno dei seguenti segnali: `SIGHUP`, `SIGINT`, `SIGTERM`, `SIGQUIT` e `SIGWINCH` (nel sistema operativo **FreeBSD** la modifica delle dimensioni della finestra del terminal comporta l'invio del segnale `SIGWINCH`). Sarebbe meglio di non interrompere il processo di eliminazione senza necessità o, se è necessario, farlo il prima possibile.

2. Dopo (nel caso di eliminazione del **Server** installato con SO **Solaris**) si deve confermare l'intenzione di eliminare il software e confermare la necessità di eseguire gli script di eliminazione dal nome dell'amministratore.

All'eliminazione del **Server** (nei sistemi operativi **FreeBSD** e **Linux**) i processi di server verranno automaticamente arrestati, il database, i file delle chiavi e i file di configurazione verranno copiati in SO **Linux** nella cartella impostata `${HOME}/drwcs/` (di solito è `/root/drwcs/`). Nel SO **FreeBSD** si propone di scegliere il percorso, quello predefinito - in `/var/tmp/drwcs`.

Nel sistema operativo **Solaris** dopo l'eliminazione del **Server** il database, i file delle chiavi e i file di configurazione verranno copiate nella cartella `/var/tmp/DrWebES`.

***Per eliminare il plugin Dr.Web Browser-Plugin:***

Eseguire il seguente comando:

- per pacchetti **deb**:
  ```
  dpkg -P drweb-esuite-plugins
  ```
- per pacchetti **rpm**:
  ```
  rpm -e drweb-esuite-plugins
  ```
- per altri sistemi (pacchetti **tar.bz2** e **tar.gz**):
  ```
  rm -f <cartella_plugin>/libnp*.so
  ```
  Per esempio, per il browser Mozilla Firefox:
  ```
  rm -f /usr/lib/mozilla/plugins/libnp*.so
  ```

## 2.7.4. Eliminazione del Proxy

## Eliminazione del Proxy per SO Windows



All'eliminazione del **Proxy** si rimuove il file di configurazione `drwcsd-proxy.xml`. Se necessario, salvare il file di configurazione manualmente prima dell'eliminazione del **Proxy**.

L'eliminazione del software del **Proxy** si esegue dagli strumenti standard del SO Windows con elemento del **Pannello di controllo** → **Installazione applicazioni** (**Applicazioni e componenti** su SO Windows 2008).

## Eliminazione del Proxy per i SO della famiglia UNIX

***Per eliminare il Proxy, eseguire:***

| Per il Proxy in | | Comando |
|---|---|---|
| SO FreeBSD | | `pkg_delete drweb-esuite-proxy` |
| SO Solaris | | `pkgrm DWEBespxy` |
| SO Linux | pacchetto deb | `dpkg -P drweb-esuite-proxy` |
| | pacchetto rpm | `rpm -e drweb-esuite-proxy` |
| | pacchetto generic | Eliminare manualmente file dalla cartella di installazione del **Proxy**. |

# Capitolo 3. Componenti di rete antivirus e la loro interfaccia

## 3.1. Dr.Web Enterprise Server

Rete antivirus deve contenere almeno un **Enterprise Server**.



Per aumentare affidabilità e produttività di rete antivirus, nonché per distribuire il carico, **Dr.Web ESS** permette di creare la rete antivirus con più **Server**. In questo caso il software di server viene installato su più computer contemporaneamente.

**Dr.Web Enterprise Server** - il servizio, che continuamente risiede nella memoria operativa. Il software di **Enterprise Server** è elaborato per i vari SO (per la lista completa delle versioni supportate dei SO v. Allegato A).

### Funzionalità principali

***Dr.Web Enterprise Server esegue le seguenti funzionalità:***

- inizializzazione di installazione di pacchetti antivirus su computer scelto o su un gruppo di computer,
- richiesta del numero della versione del pacchetto antivirus, nonché dei dati di creazione e dei numeri delle versioni di database dei virus su ogni computer protetto,
- aggiornamento dei contenuti della cartella di installazione centralizzata e della cartella di aggiornamenti,
- aggiornamento di database dei virus e dei file eseguibili dei pacchetti antivirus, nonché dei file eseguibili di componenti di rete antivirus su computer protetti.

# Raccolta informazioni sullo stato di rete antivirus

**Enterprise Server** permette di raccogliere e di fare il logging delle informazioni su operazione dei pacchetti antivirus, trasmessegli via il software dei computer protetti **(Enterprise Agent,** per più informazioni v. sotto). Il logging viene eseguito in log generale di eventi, realizzato nel formato di database. Nella rete di dimensione insignificante (non più di 200-300 computer) per gestire il log generale di eventi può essere utilizzato il database interno. Per la manutenzione di rete grandi è prevista la possibilità di utilizzare i database esterni.



Utilizzo del database interno è ammissibile alla connessione al **Server** di meno di 200-300 workstation. Se lo permette la configurazione hardware del computer, su cui è installato **Enterprise Server**, e il carico di altri processi, eseguiti su questo computer, si possono connettere fino a 1000 workstation.

Nel caso contrario si deve utilizzare il database esterno.

Se si utilizza il database esterno e al **Server** si connettono più di 10000 workstation si consiglia di eseguire i seguenti requisiti minimi:

- processore con frequenza 3 GHz,
- memoria operativa - da 4 GB per **Enterprise Server,** da 8 GB – per il server di database,
- SO della famiglia UNIX.

***Nel log generale di eventi si deve eseguire la raccolta e il logging delle seguenti informazioni:***

- informazione sulla versione dei pacchetti antivirus su computer protetti,
- ora e data di installazione e di aggiornamento del software di workstation antivirus con indicazione della versione del software,
- ora e data di aggiornamento dei database dei virus con indicazione di loro versioni,
- informazione sulla versione del SO, installata su computer

protetti, sul tipo di processore, location di cartelle di sistema del SO ecc,

- configurazione e modalità di operazione dei pacchetti antivirus (utilizzo di strumenti euristici, lista dei tipi di file scansionati, azioni al rilevamento dei virus ecc),
- informazioni su eventi dei virus, compreso il nome del virus rilevato, data di rilevamento, azioni eseguite, il risultato di cura ecc.

**Enterprise Server** avvisa l'amministratore della rete antivirus su origine di eventi, connesse all'operazione della rete antivirus per posta elettronica o con utilizzo di strumenti broadcast standard dei sistemi operativi Windows. Configurazione di eventi, che richiamano l'invio di avviso, e di altri parametri di avvisi, è descritta in Configurazione avvisi.

## Interfaccia

**Enterprise Server** non ha interfaccia incorporata. I comandi di base di gestione del **Server** sono riportati nella cartella Gestione Server.

Gestione di **Enterprise Server**, di solito, viene eseguita con il **Centro gestione**, che serve da interfaccia esterna di **Server**.

## Avvio e arresto di Dr.Web Enterprise Server

Di default **Enterprise Server** viene avviato automaticamente dopo l'installazione e dopo ogni riavvio del sistema operativo.

Si può avviare, riavviare o arrestare **Enterprise Server** in uno dei seguenti modi:

***Per i SO della famiglia UNIX***

- Con il comando corrispondente di console (v. anche Allegato H5. Dr.Web Enterprise Server):
  - Avvio:

- per il SO FreeBSD:
  ```
  # /usr/local/etc/rc.d/drwcsd.sh start
  ```
- per i SO Linux e Solaris:
  ```
  # /etc/init.d/drwcsd start
  ```

○ Riavvio:

- per il SO FreeBSD:
  ```
  # /usr/local/etc/rc.d/drwcsd.sh restart
  ```
- per i SO Linux e Solaris:
  ```
  # /etc/init.d/drwcsd restart
  ```

○ Arresto:

- per il SO FreeBSD:
  ```
  # /usr/local/etc/rc.d/drwcsd.sh stop
  ```
- per i SO Linux e Solaris:
  ```
  # /etc/init.d/drwcsd stop
  ```

◆ Arresto e riavvio via il **Centro gestione**:

- Nella sezione **Amministrazione**: riavvio con il tasto  , arresto con il tasto  (manca nella versione per il SO Solaris).

### *Per il SO Windows*

◆ Caso generale:

- Con il comando corrispondente, locato nel menu **Start** → **Programmi** → **Dr.Web Enterprise Server**.
- Con gli strumenti di gestione dei servizi nella sezione **Amministrazione** del **Pannello di controllo** del SO Windows.

◆ Arresto e riavvio via il **Centro gestione**:

- Nella sezione **Amministrazione**: riavvio con il tasto  , arresto con il tasto  .

◆ Con i comandi di console, eseguiti da sottocartella `bin` della cartella di installazione del **Server** (v. anche Allegato H5. Dr.Web Enterprise Server):

- `drwcsd start` — avvio del **Server**.

- `drwcsd restart` — riavvio completo del servizio del **Server**.
- `drwcsd stop` — completamento regolare di operazione del **Server**.

# 3.2. Dr.Web Enterprise Agent

## Principio di operazione

Protezione antivirus di workstation viene eseguita dai pacchetti antivirus di **Dr.Web**, sviluppati per i SO corrispondenti.

Nei contenuti di **Dr.Web Antivirus ESS** questi pacchetti operano sotto gestione di **Enterprise Agent**, installato su computer protetto e continuamente caricato nella memoria. Con supporto di connessione a **Enterprise Server**, l'amministratore può configurare **Antivirus** nel modo centralizzato su workstation con il **Centro gestione**, impostare orario di controlli antivirus, visualizzare le statistiche ed altre informazioni su operazione dei componenti antivirus, avviarli e arrestare la scansione antivirus ecc.

**Enterprise Server** carica aggiornamenti e li trasmette ad **Agent** connessi. In questo modo con **Enterprise Agent** si installa, si supporta e si regola la strategia ottima di protezione dai virus nonostante il livello di qualifica di utenti di workstation.

Comunque nel caso di disconnessione provvisoria di workstation da rete antivirus, **Enterprise Agent** utilizza la copia locale delle configurazioni, protezione antivirus su workstation mantiene la sua funzionalità (durante il periodo che non supera il periodo di validità di licenza di utente), ma aggiornamento dei database dei virus e del software non viene eseguito.

Aggiornamento di **Agent** mobili è descritto in Aggiornamento di Agent mobiliDr.Web Enterprise Agent.

## Funzioni principali

***Dr.Web Enterprise Agent realizza le seguenti funzioni:***

- esegue installazione, aggiornamento e configurazione del pacchetto antivirus di **Dr.Web**, avvio di scansione, nonché esecuzione di altri processi, creati da **Enterprise Server**;
- permette di richiamare i componenti del pacchetto antivirus di **Dr.Web** via l'interfaccia speciale;
- trasmette i risultati di esecuzione di processi a **Enterprise Server**;
- trasmette a **Enterprise Server** degli avvisi su origine di eventi precedentemente specificati nell'operazione del pacchetto antivirus.

Ogni **Enterprise Agent** è connesso a **Enterprise Server** e fa parte di uno o più gruppi, registrati su questo **Server** (per più informazioni v. Gruppi di sistema e di utente). Trasmissione delle informazioni tra **Agent** e **Server** indicato è eseguito via il protocollo, utilizzato nella rete locale (TCP/IP, IPX o NetBIOS).



Di seguito il computer protetto con **Agent** installato, secondo le sue funzioni nella rete antivirus, sarà denominato *workstation* antivirus. Si deve ricordare che secondo le sue funzioni nella rete antivirus tale computer può essere sia workstation, sia server della rete locale.

## Interfaccia di gestione nel SO Windows

**Enterprise Agent** avviato nell'ambito del SO visualizza nell'area di notifica nella barra delle applicazioni l'icona  .

I tipi disponibili di icona di **Agent** e stati di componenti corrispondenti sono riportati in tabella 3-1.

**Tabella 3-1. I tipi disponibili di icona e lo stato di componenti corrispondente**

| Icona | Descrizione | Stato |
|---|---|---|
|  | Immagine nero sullo sfondo verde. | **Agent** opera regolarmente e si connette al **Server**. |
|  | Frecce rosse nello sfondo di icona. | Manca connessione al **Server**. |
|  | Il punto esclamativo nel triangolo giallo nello sfondo di icona. | **Agent** richiede il riavvio del computer o sono disattivati i componenti **SelfPROtect** o **Spider Guard** |
|  | Lo sfondo di icona cambia il colore dal verde al rosso. | È successo un errore in aggiornamento dei componenti di pacchetto. |
|  | Lo sfondo di icona è continuamente rosso. | **Agent** è arrestato o non opera. |
|  | Lo sfondo di icona è giallo. | **Agent** opera nella modalità mobile. Per più informazioni v. Aggiornamento di Agent mobili Dr.Web Enterprise Agent |

Alcune funzioni di gestione di **Agent** e di componenti antivirus su workstation sono disponibili via il menu contestuale dell'icona di **Agent,** rappresentata in immagine 3-1.




**Immagine 3-1. Menu contestuale di Enterprise Agent**

Le configurazioni, disponibili tra il menu contestuale di **Agent**, dipendono dalla configurazione di workstation, impostata su **Enterprise Server**, nonché dei diritti di utente su workstation.

Contenuti dei parametri di **Enterprise Agent**, del pacchetto antivirus e la descrizione delle funzioni corrispondenti per gestire workstation sono riportati nella guida di **Enterprise Agent**.

Informazione sulle configurazioni di **Enterprise Agent**, impostate via **Enterprise Server**, sono riportate in Configurazione di Dr.Web Enterprise Agent.

## Avvio e arresto di Dr.Web Enterprise Agent nel SO Windows



Comando **Uscire** nel menu contestuale di **Agent** arresta l'operazione solamente di GUI di **Agent** (v. Interfaccia di gestione nel SO Windows) ed elimina l'icona dall'area di notifica di barra delle applicazioni. **Agent** in questo caso continua ad operare.

Per arrestare l'operazione dello stesso **Agent**, eseguire nella riga di comando:

```
net stop drwagntd
```

Si sconsiglia di arrestare **Agent**, perché in questo caso il software del pacchetto antivirus non viene aggiornato, e **Server** non ottiene le informazioni sullo stato di workstation, anche se in questo caso la protezione costante del computer non viene disattivata.

**Agent** viene automaticamente avviato dopo il riavvio del computer. Per avviare **Agent** senza riavviare il computer, eseguire nella riga di comando:

```
net start drwagntd
```

# 3.3. Centro gestione di Dr.Web

Per gestire la rete antivirus in generale (compreso la modifica dei suoi contenuti e della sua struttura), tutti i suoi componenti, nonché per la configurazione di **Enterprise Server** si utilizza il **Centro gestione** di **Dr.Web**.



Per operazione corretta **Centro gestione** nel browser web Windows Internet Explorer nelle configurazioni del browser web si deve aggiungere l'indirizzo del **Centro gestione** alla zona affidata: **Strumenti** → **Opzioni Internet** → **Sicurezza** → **Siti attendibili**.

Per operazione corretta del **Centro gestione** nel browser web Chrome si devono disattivare i cookies nelle configurazioni di browser web.

## Connessione a Dr.Web Enterprise Server

Su un computer che ha accesso a **Enterprise Server**, il **Centro gestione** è disponibile all'indirizzo:
`http://`*<Indirizzo_Server>*`:9080`

o
`https://`*<Indirizzo_Server>*`:9081`

dove come *<Indirizzo_Server>* indicare indirizzo IP o nome di dominio del computer, su cui è installato **Enterprise Server**.



Ci sono diversi Numeri porte per connessione via http e per la connessione protetta via https: `9080` e `9081` rispettivamente.

Nella finestra di dialogo di richiesta di autorizzazione inserire il nome e la password dell'amministratore (nome di amministratore predefinito con i diritti completi – **admin**, password – password, che è stato impostato all'installazione del **Server**).

Durante il carico via https (connessione protetta con SSL), browser richiede la conferma del certificato, utilizzato dal **Server**. In questo caso la richiesta di conferma può indicare la non affidabilità del certificato e presumono la sua non validità. Tali informazioni vengono visualizzati all'utente perché il certificato è sconosciuto al browser. Per poter caricare il **Centro gestione** si deve accettare il certificato proposto.

Altrimenti il carico non è possibile.



In alcune versioni del browser, per esempio, **FireFox 3** e superiori, al carico via https va in errore, e il **Centro gestione** non viene caricato. In questo caso sulla pagina di errore si deve scegliere la voce **Aggiungere sito alla lista esclusioni** (sotto il messaggio di errore). Dopodiché è consentito l'accesso al **Centro gestione**.

## Interfaccia del Centro gestione di Dr.Web

Finestra del **Centro gestione** (v. immagine 3-2) è suddivisa in *intestazione* e in *area operativa*.

*Intestazione* contiene:

- logo del prodotto **Dr.Web Enterprise Security Suite**: se si preme, si apre la finestra principale del **Centro gestione** (corrisponde a scelta della voce **Rete antivirus** del menu principale),
- menu principale,
- nome di utenza dell'amministratore, sotto cui si è accessi al **Centro gestione**,
- tasto **Esci** per completare la sessione attuale di operazione con il **Centro gestione**.



Se nel **Centro gestione** è attivata autorizzazione automatica, se si preme il tasto **Esci**, le informazioni su nome e password dell'amministratore vengono eliminati.

All'entrata successiva nel **Centro gestione** si deve ripetere la procedura standard di autorizzazione, indicando nome e password. In questo caso, se è attiva autorizzazione automatica, nome e password indicati si salvano in questo browser web e autorizzazione nel **Centro gestione** avviene automaticamente (senza input di nome e password) finché non si prema di nuovo il tasto **Esci**.

*Area operativa* provvede alla funzionalità principale del **Centro gestione**. Consiste di due o tre pannelli, secondo le azioni eseguite. In questo caso si implementa l'innestazione della funzionalità dei pannelli da sinistra a destra:

- *menu di gestione* è sempre locato nella parte sinistra della finestra,
- secondo la voce, scelto nel menu di gestione, si visualizzano una o due pannelli aggiuntivi. Nell'ultimo caso, nella parte destra si visualizzano le proprietà o le configurazioni di elementi del pannello centrale.

La lingua di interfaccia si imposta separatamente per ogni utenza dell'amministratore (v. Gestione utenze amministratori).

## *Menu principale*

Nel menu principale del **Centro gestione** sono disponibili le seguenti voci:

- Amministrazione,
- Rete antivirus,
- Impostazioni,
- Legami,
- Aiuto,
- e Barra di ricerca.




**Immagine 3-2. Finestra del Centro gestione di Dr.Web. Premere sulla voce del menu principale per passare alla descrizione**

## *Barra di ricerca*

Per semplificare la ricerca di un elemento richiesto si utilizza la *barra di ricerca,* locata nel destro confine del menu principale del **Centro gestione**. La barra permette di eseguire la ricerca sia di gruppi, sia di workstation singoli secondo i parametri indicati.

### *Per cercare workstation o gruppi di workstation:*

1. Nella lista a cascata della barra di ricerca scegliere criteri di ricerca:
   - **Postazione** - per ricercare workstation per nome,
   - **Gruppo** - per ricercare gruppi per nome,
   - **ID** - per ricercare gruppi e workstation secondo identificatori unici,
   - **Descrizione** - per ricercare gruppi e workstation per la loro descrizione,
   - **Indirizzo IP** - per ricercare workstation per indirizzo IP.
2. Inserire una riga, secondo la quale verrà eseguita la ricerca. Si

possono impostare:

- una riga concreta per una completa corrispondenza con il parametro della ricerca,
- una maschera di riga ricercata: sono ammessi i caratteri ***** e **?**.

3. Premere il tasto ENTER per far partire una ricerca.
4. Nella lista gerarchica saranno visualizzati tutti gli elementi, trovati secondo i parametri di ricerca, e in questo caso:
   - se è stata eseguita una ricerca di workstation, saranno visualizzate tutte le appartenenze di workstation a tutti i gruppi,
   - se come il risultato di ricerca non è stato rilevato nessun elemento, viene visualizzata lista gerarchica vuota con messaggio **Nessun risultato della ricerca**.

Si può inoltre utilizzare l'opzione **Ricerca avanzata**.

***Per una ricerca avanzata eseguire le seguenti azioni:***

1. Premere sul tasto  nella barra di ricerca.
2. Nella barra aperta **Ricerca dei gruppi e delle postazioni** indicare i seguenti parametri:
   - **Nome della postazione** - inserire una riga, secondo la quale viene eseguita le ricerca per nomi di workstation.
   - **Nome del gruppo** - inserire una riga, secondo la quale viene eseguita le ricerca per nomi dei gruppi.
   - **ID** - inserire una riga, secondo la quale viene eseguita le ricerca per identificatori unici di gruppi e di workstation.
   - **Indirizzo IP della postazione** - inserire una riga, secondo la quale viene eseguita le ricerca per indirizzi IP di workstation.
   - **Descrizione** - impostare una riga di descrizione, secondo la quale verrà eseguita la ricerca di elemento.

   Si possono impostare i valori di uno, di più o di tutti i campi di ricerca avanzata.

   Se si impostano più campi, viene eseguita la ricerca di tutti gli

elementi che soddisfino almeno un criterio di quelli impostati (i valori di ricerca si uniscono sulla base di ricerca secondo il metodo *O*).

3. Dopo aver impostato i valori dei campi di ricerca necessari, premere sul tasto **Trova**.
4. Nella lista gerarchica saranno visualizzati tutti gli elementi trovati o il messaggio **Nessun risultato della ricerca**.

## 3.3.1. Amministrazione

Scegliere nel menu principale del **Centro gestione** la voce **Amministrazione**. Per visualizzare e modificare le informazioni nella finestra aperta utilizzare il menu di gestione, locato nella parte sinistra della finestra.

***Il menu di gestione contiene le seguenti voci:***

1. **Amministrazione**
   - **Dr.Web Enterprise Server** — apre il pannello, con cui si possono visualizzare le informazioni principali del **Server**, nonché riavviarlo con il tasto  o arrestarlo con il tasto  (assente nella versione per i SO Solaris), locati nella parte destra superiore del pannello;
   - **Postazioni non confermate** — apre il pannello con la lista di workstation non confermate (v. Politica di connessione workstation);
   - **Manager licenze** — permette di gestire i file chiavi di licenza del **Server** e di **Agent** (v. Gestore licenze);
   - **Chiavi di crittografia** — permette di esportare (salvare localmente) chiavi di codifica aperta e chiusa.
2. **Tabelle**
   - **Log di verifica** — visualizzazione del log di eventi e delle modifiche, eseguite con il **Centro gestione**;
   - **Log di verifica esecuzione dei task** — contiene la lista di processi impostati sul **Server** con nota di esecuzione e con commenti;

- **Statistiche del server** — contiene le statistiche di operazione di questo **Server**.

3. **Configurazione**
   - **Amministratori** — apre il pannello di controllo di utenze degli amministratori di rete antivirus (v. Gestione utenze amministratori);
   - **Autorizzazione** — apre il pannello di gestione di autenticazione di amministratori nel **Centro gestione** (v. Autenticazione di amministratori);
   - **Stato del repository** — permette di controllare lo stato di repositorio: la data dell'ultimo aggiornamento dei componenti del repositorio e il loro stato (v. Stato repositorio);
   - **Configurazione del repository** — apre la finestra di editor del repositorio (v. Editor configurazione repositorio);
   - **Configurazione Dr.Web Enterprise Server** — apre il pannello di impostazioni principali del **Server** (v. Configurazione di Dr.Web Enterprise Server);
   - **Orario Dr.Web Enterprise Server** — apre il pannello di configurazione orario di processi del **Server** (v. Configurazione orario di Dr.Web Enterprise Server);
   - **Editor dei template** — apre la finestra di editori di moduli di avvisi (v. Configurazione avvisi).

4. **Installazione**
   - **Scanner di rete** — permette di impostare la lista delle reti ed eseguire sia la scansione delle reti per la presenza del software antivirus installato, provvedendo allo stato protetto dei computer, sia l'installazione dell'ultimo (v. Scanner di rete);
   - **Installazione per la rete** — permette di semplificare l'installazione del software di **Agent** su workstation antivirus concrete (v. Installazione di Dr.Web Enterprise Agent con utilizzo del Centro gestione Dr.Web).

## 3.3.2. Rete antivirus

Scegliere nel menu principale del **Centro gestione** la voce **Rete antivirus**. Per visualizzare e modificare le informazioni nella finestra aperta si utilizza il menu di gestione, locato nella parte sinistra della finestra.

### *Lista gerarchica*

Nella parte centrale della finestra è locata la lista gerarchica di rete antivirus. La lista gerarchica (il catalogo) della rete antivirus rispecchia la struttura ad albero di elementi della rete antivirus. I nodi di questa struttura sono i gruppi e le workstation che ne fanno parte.

***Si possono applicare le seguenti azioni agli elementi della lista:***

- premere con il tasto sinistro del mouse su un nome di gruppo o di workstation per visualizzare il menu di gestione (nella parte sinistra della finestra) di elemento corrispondente;
- premere con il tasto sinistro del mouse su icona di un gruppo per visualizzare i contenuti del gruppo.



Per scegliere più workstation o gruppi della lista gerarchica scegliere con il mouse tenendo premuti i tasti CTRL o SHIFT.

Il tipo di icona di elemento della lista dipende dal tipo o dallo stato di tale elemento (v. tabella 3-2).

**Tabella 3-2. Icone di elementi della lista gerarchica**

| Icona | Descrizione | Valore |
|---|---|---|
| | | **Gruppi** |
|  | cartella gialla | Gruppi, visualizzati sempre nella lista gerarchica. |
|  | cartella bianca | La visualizzazione dei gruppi nella lista gerarchica può essere disattivata, se i gruppi sono vuoti. |
| | | **Workstation** |
|  | icona verde | Workstation disponibile con il software antivirus installato. |
|  | icona grigia | Workstation non disponibile. |
|  | icona barrata | Software antivirus su workstation è disinstallato. |



Se sono impostate le configurazioni personalizzate per workstation o gruppo (se nel gruppo ci sono workstation con le configurazioni personalizzate), nella lista gerarchica su icona di tale gruppo o workstation viene visualizzata icona. Per esempio, se le configurazioni personalizzate sono impostate per workstation disponibile con il software antivirus installato, la sua icona avrà il seguente aspetto: .

Per visualizzare le icone con le configurazioni personalizzate scegliere la voce **Impostazioni del tipo albero** nella barra degli strumenti o mettere il flag **Visualizza le impostazioni individuali**.

La gestione di elementi del catalogo della rete antivirus è eseguita con la barra degli strumenti della lista gerarchica.

## *Barra degli strumenti*

La barra degli strumenti della lista gerarchica contiene i seguenti elementi:

**Generali**. Permette di gestire parametri generali della lista gerarchica. Scegliere la voce corrispondente nella lista a cascata:

**Rimuovere gli oggetti segnalati**. Permette di eliminare oggetti della lista gerarchica. Per farlo, scegliere nella lista un elemento o più elementi e premere su **Eliminare oggetti scelti**.

**Modificare**. Apre la barra delle proprietà workstation o gruppo nella parte destra della finestra del **Centro gestione**.

**Impostare questo gruppo come primario**. Permette di impostare un gruppo scelto nella lista gerarchica come primario per tutte le workstation che ne fanno parte.

**Impostare il gruppo primario**. Permette di impostare per workstation scelte nella lista un gruppo primario. In questo caso, se nella lista gerarchica è scelto un gruppo, per tutte le workstation che ne fanno parte sarà impostato il gruppo primario scelto.

**Unire le postazioni**. Permette di unire workstation sotto un'unica utenza nella lista gerarchica. Si utilizza se la stessa workstation è stata registrata sotto le utenze diverse (v. Unione workstation).

**Rimuovere le impostazioni individuali dell'oggetto**. Permette di eliminare le configurazioni personalizzate di un oggetto scelto nella lista. In questo caso, le configurazioni saranno ereditate dal gruppo primario. Se nella lista gerarchica è scelto un gruppo, saranno cancellate le configurazioni di tutte le workstation che ne fanno parte.

**Importo della chiave**. Permette di impostare la chiave per workstation o gruppo.

**Inviare messaggi alle postazioni**. Permette di avviare a utenti un avviso con qualsiasi contenuto (v. Invio avvisi a utenti).

**Disinstalla Dr.Web Enterprise Agent**. Elimina l'**Agent** e il

software antivirus da una workstation scelta o da un gruppo di workstation.

**Installa Dr.Web Enterprise Agent**. Apre Scanner di rete per installare **Agent** su workstation scelte. Questa voce è attiva solo se si scelgono workstation confermate nuove o workstation con **Agent** disinstallato.

**Ripristinare le postazioni rimosse**. Permette di ripristinare le workstation eliminate in precedenza (v. anche Eliminazione e ripristino workstation). Questa voce è attiva solo se si scelgono workstation dal sottogruppo **Eliminate** nel gruppo **Stato**.

**Si può aggiungere uno postazione o un gruppo**. Permette di creare un nuovo elemento di rete antivirus. Per farlo, scegliere la voce corrispondente nella lista a cascata:

**Creare postazione**. Permette di creare una nuova workstation (v. Creazione nuova utenza).

**Creare gruppo**. Permette di creare un nuovo gruppo (v. Creazione e eliminazione gruppi).

**Esportare dati**. Permette di scrivere i dati comuni su workstation di rete antivirus nel file del formato CSV, HTML o XML. Il formato di esportazione richiesto è scelto nella lista a cascata.

**Impostare la visualizzazione del gruppo**. Permette di modificare i parametri di visualizzazione gruppi. Per farlo, scegliere un gruppo nella lista a cascata e indicare nella lista a cascata una delle seguenti varianti (in questo caso si modifica l'icona del gruppo, v. tabella 3-2):

**Nascondere il gruppo** - visualizzazione del gruppo nella lista gerarchica è sempre disattivata.

**Nascondere se vuoto** - visualizzazione del gruppo nella lista gerarchica è disattivata se il gruppo è vuoto (non contiene workstation).

**Mostrare** - il gruppo è sempre visualizzato nella lista gerarchica.

**Gestione dei componenti**. Permette di gestire componenti antivirus su workstation. Per farlo, scegliere nella lista a cascata una

delle seguenti varianti:

 **Aggiornare tutti i componenti**. Prescrive di aggiornare tutti i componenti di antivirus installati, per esempio, nella situazione quando **Agent** non si è connesso al **Server** per un lungo periodo (v. Aggiornamento manuale dei componenti di Dr.Web Enterprise Security Suite);

 **Aggiornare componenti falliti**. Prescrive un aggiornamento forzato dei componenti, il cui aggiornamento è andato in errore;

 **Interrompere quelli avviati**. Prescrive di arrestare le scansioni avviate su workstation. La descrizione completa di procedura di arresto di scansioni per tipi è riportata in Arresto operazione componenti avviati per tipi.

 **Scansionare**. Permette di eseguire la scansione di workstation in modalità, scelta nella lista a cascata (v. anche Avvio scansione workstation):

 **Dr.Web Scanner per Windows. Scansione rapida**. In questa modalità si esegue la scansione dei seguenti oggetti:

- memoria operativa,
- settori di avvio di tutti i dischi,
- oggetti di autoesecuzione,
- cartella radice del disco di avvio,
- cartella radice del disco di installazione del SO Windows,
- cartella di sistema del SO Windows,
- cartella `Miei documenti`,
- cartella temporanea di sistema,
- cartella temporanea dell'utente.

 **Dr.Web Scanner per Windows. Scansione completa**. In questa modalità si esegue la scansione completa di tutti i dischi rigidi e di tutti i dispositivi rimovibili (compresi i settori di avvio).

 **Dr.Web Scanner per Windows. Scansione personalizzata**. Questa modalità permette di scegliere qualsiasi file o cartella per la successiva scansione.

 **Dr.Web Enterprise Scanner per Windows**. In questa

modalità si esegue la scansione personalizzata con **Dr.Web Enterprise Scanner**.

**Dr.Web Enterprise Scanner per Mac OS X**. Per scansionare secondo i parametri di scansione impostati, computer che funzionano sotto i SO della famiglia Mac OS X.

**Dr.Web Enterprise Scanner per Unix**. Per scansionare secondo i parametri di scansione impostati, computer che funzionano sotto i SO della famiglia UNIX.

**Impostazioni del tipo albero** permettono di modificare aspetto esterno della lista:

- per gruppi:
  - **Appartenenza a tutti i gruppi**. Imposta il doppiaggio di workstation nella lista, se essa fa parte di più gruppi (solo per gruppi con icona di cartella bianca - v. tabelle 3-2). Se il flag è posto - saranno visualizzati tutte le appartenenze di workstation. Se è tolto - workstation viene visualizzata nella lista una sola volta.
  - **Mostra i gruppi nascosti**. Per visualizzare tutti i gruppi, che fanno parte di rete antivirus. Se si toglie questo flag, i gruppi vuoti (che non contengono workstation) saranno nascosti. Questo può essere utile per escludere le informazioni eccessive, per esempio, se ci sono tanti gruppi vuoti.
- per workstation:
  - **Mostra l'identificatore della postazione**. Imposta visualizzazione di workstation nella lista gerarchica per identificatori unici.
  - **Mostra il nome della postazione**. Imposta visualizzazione dei nomi (denominazioni) workstation, se tali sono impostati.
  - **Mostra l'indirizzo della postazione**. Imposta visualizzazione di workstation nella lista gerarchica per indirizzi IP.
  - **Mostra il server delle postazioni**. Imposta visualizzazione dei nomi o di indirizzi di **Server** antivirus, a cui sono connesse le workstation.

- per tutti elementi:
  - **Visualizza le impostazioni individuali**. Attiva/disattiva indicatore su icone di workstation o di gruppi, che segnala presenza delle configurazioni personalizzate.
  - **Mostra descrizioni**. Attiva/disattiva visualizzazione descrizioni gruppi e workstation (descrizioni si impostano nelle proprietà di elementi).
  - **Mostra il numero di postazioni**. Attiva/disattiva visualizzazione numero workstation per tutti i gruppi di rete antivirus.

### *Barra delle proprietà*

La barra delle proprietà serve per visualizzare le proprietà e le configurazioni di workstation e gruppi.

***Per visualizzare la barra delle proprietà:***

1. Nella lista gerarchica scegliere una workstation o un gruppo e premere su **Generali** → **Modificare** nella barra degli strumenti.
2. Nella parte destra della finestra del **Centro gestione** si apre la barra con le proprietà di workstation. Questa barra contiene i seguenti gruppi di configurazioni: **Generali**, **Configurazione**, **Gruppi**, **Posizione**. La descrizione completa di queste configurazioni è riportata in Configurazione workstation.

## 3.3.3. Impostazioni

Scegliere nel menu principale del **Centro gestione** la voce **Impostazioni**.



Tutte le configurazioni di questa sezione sono validi solo per utenza attuale dell'amministratore.

Il menu di gestione, locato nella parte sinistra della finestra, contiene i seguenti elementi:

- **Il mio account**.
- **Interfaccia**.

## *Il mio account*

Con questa sezione si gestisce l'utenza attuale dell'amministratore di rete antivirus (v. anche Gestione utenze amministratori).

> I valori dei campi, marcati con il carattere *, sono obbligatori da impostare.

Se necessario, modificare i seguenti parametri:

- **Nome di registrazione** dell'amministratore - login per accedere al **Centro gestione**.
- Mettere il flag **Solo lettura** per limitare i diritti di accesso.
- Nome e cognome dell'amministratore.
- **Lingua d'interfaccia**, utilizzata da questo amministratore.
- **Formato della data**, utilizzato da questo amministratore durante la modifica di configurazioni, che contengono le date. Sono disponibili le seguenti formati:
  - europeo: GG-MM-AAAA OO:MM:SS
  - americano: MM/GG/AAAA OO:MM:SS
- **Descrizione** di utenza.
- Per l'utenza dell'amministratore dei gruppi mettere il flag **Può amministrare un numero di gruppi limitato** per impostare i gruppi disponibili.
- Per modificare la password premere sul tasto **Nuova password** nella barra degli strumenti.

I seguenti parametri sono di sola lettura:

- Data creazione utenza e ultima modifica dei suoi parametri,

- **Stato** - visualizza l'indirizzo di rete di ultima connessione sotto questa utenza.

Dopo la modifica dei parametri premere sul tasto **Salva**.

Per le utenze con i diritti di sola lettura si possono modificare solamente i seguenti campi:

- **Lingua di interfaccia**,
- **Descrizione**.

## *Interfaccia*

### *Configurazioni ad albero*

I parametri di questa sottosezione permettono di modificare l'aspetto esterno della lista e sono simili alle configurazioni, locate nella barra degli strumenti della voce  nella sezione del menu principale **Rete antivirus**:

- per gruppi:
  - **Appartenenza a tutti i gruppi**. Imposta il doppiaggio di workstation nella lista, se essa fa parte di più gruppi (solo per gruppi con icona di cartella bianca - v. tabelle 3-2). Se il flag è posto - saranno visualizzati tutte le appartenenze di workstation. Se è tolto - workstation viene visualizzata nella lista una sola volta.
  - **Mostra i gruppi nascosti**. Per visualizzare tutti i gruppi, che fanno parte di rete antivirus. Se si toglie questo flag, i gruppi vuoti (che non contengono workstation) saranno nascosti. Questo può essere utile per escludere le informazioni eccessive, per esempio, se ci sono tanti gruppi vuoti.
- per workstation:
  - **Mostra l'identificatore della postazione**. Imposta visualizzazione di workstation nella lista gerarchica per identificatori unici.

- **Mostra il nome della postazione**. Imposta visualizzazione dei nomi (denominazioni) workstation, se tali sono impostati.
- **Mostra l'indirizzo della postazione**. Imposta visualizzazione di workstation nella lista gerarchica per indirizzi IP.
- **Mostra il server della postazione**. Imposta visualizzazione dei nomi o di indirizzi di **Server** antivirus, a cui sono connesse le workstation.

◆ per tutti elementi:

- **Visualizza le impostazioni individuali**. Attiva/disattiva indicatore su icone di workstation o di gruppi, che segnala presenza delle configurazioni personalizzate.
- **Mostra descrizioni**. Attiva/disattiva visualizzazione descrizioni gruppi e workstation (descrizioni si impostano nelle proprietà di elementi).

### *Scanner di rete*



Per operazione di **Scanner di rete** è necessario che sia installato il plugin Dr.Web Browser-Plugin

I parametri di questa sottosezione permettono di impostare le configurazioni di Scanner di rete predefinite.

Per avviare lo **Scanner di rete** stesso scegliere nel menu principale del **Centro gestione** la voce **Amministrazione**, nel menu di gestione (pannello a sinistra) scegliere la voce **Scanner di rete**.

Impostare i seguenti parametri di **Scanner di rete**:

1. Nel campo di input **Reti** impostare la lista di reti nel formato:
   - con utilizzo di trattino (per esempio, `10.4.0.1-10.4.0.10`),
   - separati di virgola e spazio (per esempio, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
   - separati da prefisso di rete (per esempio, `10.4.0.0/24`).
2. Se necessario, modificare la **Porta** e il valore del parametro

**Time-out**.

3. Per salvare i valori predefiniti premere sul tasto **Salva**. Di seguito se si utilizza lo Scanner di reti questi parametri saranno impostati automaticamente.

### *Intervallo di tempo*

In questa sottosezione si impostano le configurazioni del periodo di tempo, nei limiti del quale si visualizzano i dati statistici (v. Visualizzazione risultati operazione e statistici consuntivi della workstation):

- Nella lista a cascata **Intervallo di lettura delle statistiche** si imposta il periodo di tempo predefinito per tutte le sezioni di dati statistici.

  Alla prima apertura della pagina le statistiche si visualizzano per il periodo di tempo indicato. Se necessario, si può modificare il periodo di tempo direttamente nelle stesse sezioni di statistiche.

- Per farsì che nelle sezioni di statistiche si salvi l'ultimo periodo impostato, mettere il flag **Salva l'ultimo intervallo di lettura delle statistiche**.

  Se il flag è posto, alla prima apertura di pagina si visualizzano le statistiche per l'ultimo periodo, scelto nel browser web.

  Se il flag è tolto, alla prima apertura di pagina si visualizzano le statistiche per il periodo, impostato nella sezione **Periodo di visualizzazione statistiche**.

### *Autorizzazione*

Mettere il flag **Autorizzazione automatica** per consentire nel browser web attuale l'autorizzazione automatica a tutti i **Centro gestione** di **Dr.Web** con il nome utente e la password dell'amministratore analoghi.

Dopo che si mette tale flag, con l'estensione di **Dr.Web Browser-Plugin** si salvano nome e password, che l'amministratore indica durante l'autorizzazione successiva nel **Centro gestione**.



Per il funzionamento di autorizzazione automatica è necessario che sia installato Dr.Web Browser-Plugin.

Di seguito, se si apre un **Centro gestione** di **Dr.Web** in questo browser web, l'autorizzazione sarà eseguita automaticamente se sul **Server** c'è un utente con questo nome e password. Se nome e password non corrispondono (per esempio, non esiste tale utente o utente con questo nome ha un'altra password), sarà visualizzata la finestra standard di autorizzazione del **Centro gestione**.



Se si preme il tasto **Esci** nell'intestazione dell'interfaccia del **Centro gestione**, si eliminano le informazioni su nome e su password dell'amministratore.

Nell'entrata successiva nel **Centro gestione** si deve ripetere la procedura standard di autorizzazione, indicando nome e password. In questo caso dopo l'autorizzazione automatica attivata, nome e password indicati si memorizzano in questo browser web, e l'autorizzazione nel **Centro gestione** viene eseguita automaticamente (senza inserire nome e password) finché non si preme successivamente sul tasto **Esci**.

## 3.3.4. Legami

Scegliere nel menu principale del **Centro gestione** la voce **Legami**. Per scegliere le informazioni visualizzate è disponibile il menu di gestione, locato nella parte sinistra della finestra.

### *Amministrazione*

La sezione **Amministrazione** del menu di gestione contiene la voce **Legami**, che serve per gestire le connessioni tra i **Server** nella rete antivirus a più server (v. Particolarità di rete con più server).

Nell lista gerarchica sono riportati tutti i **Enterprise Server**, connesse a questo **Server**.

Creazione di nuove connessioni intraserver è descritto nella sezione Configurazione connessioni tra server.

### *Tabelle*

Nella sezione **Tabelle** del menu di gestione sono riportate le informazioni sul funzionamento della rete antivirus, ottenute da altri **Server** (v. Particolarità di rete con più server).

Per visualizzare le tabelle consuntive con i dati di altri **Server** premere sulla voce corrispondente della sezione **Tabelle**.

## 3.3.5. Aiuto

Scegliere nel menu principale del **Centro gestione** la voce **Aiuto**.

Il menu di gestione, locato nella parte sinistra della finestra, contiene i seguenti elementi:

1. **Generali**
   - **Forum** - passare al forum della società **Doctor Web**.
   - **Fai una domanda** - passare alla pagina del **Supporto tecnico** di **Doctor Web**.
   - **Spedisci un virus** - aprire il modulo per l'invio di un virus al laboratorio di **Doctor Web**.
   - **wiki** - passare alla pagina di Wikipedia - database di informazioni, dedicato ai prodotti della società **Doctor Web**.
   - **Comunica un errore nel funzionamento del Parental Control** - aprire il modulo per inviare messaggio sul falso positivo o su omissione di link dannosi nel plugin **Controllo genitori**.
2. **Documentazione**
   - **Manuale dell'amministratore** - aprire la documentazione dell'amministratore nel formato HTML.
   - **Manuale dell'utente** - aprire la documentazione dell'utente nel formato HTML.

- **XML Web API** - aprire la documentazione dell'amministratore sul XML Web APInel formato HTML.
- **Note sulla versione** - aprire la sezione commenti all'edizione di **Dr.Web Enterprise Security Suite** della versione installata.

# 3.4. Componenti Centro gestione Dr.Web

## 3.4.1. Scanner di rete

Nei contenuti di **Enterprise Server** rientra **Scanner di rete**.



Non si consiglia di avviare lo **Scanner di rete** nel SO Windows 2000 e inferiori: la visualizzazione di rete può essere non completa.

Operazione di **Scanner di rete** è garantita nei SO della famiglia UNIX o nel SO Windows XP e superiori.

Per operazione di **Scanner di rete** è necessario che sia installato il plugin Dr.Web Browser-Plugin

***Scanner di rete esegue le seguenti funzioni:***

- Scansione (visualizzazione) di rete per rilevare workstation.
- Rilevamento della presenza di **Enterprise Agent** su workstation.
- Installazione di **Enterprise Agent** su workstation rilevati secondo le indicazioni dell'amministratore. Per una descrizione dettagliata di installazione di **Enterprise Agent** v. Installazione di Dr.Web Enterprise Agent con utilizzo del Centro gestione di Dr.Web.

***Per scansione (visualizzazione) di rete eseguire le seguenti azioni:***

1. Aprire la finestra di **Scanner di rete**. Per farlo, scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Scanner di rete**. Si apre la finestra di **Scanner di rete**.
2. Se necessario, mettere il flag **Scansione rapida** per eseguire la scansione nella modalità rapida.
3. Indicare nel campo di input di **Reti** la lista di reti nel formato:
   - separate da trattino (per esempio, `10.4.0.1-10.4.0.10`),
   - separate da virgola e spazio (per esempio, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`),
   - con utilizzo del prefisso di rete (per esempio, `10.4.0.0/24`).
4. Indicare la porta, via cui si deve connettersi ad **Agent**.
5. Se necessario, modificare il valore di timeout in secondi, durante il quale si aspetta una risposta da workstation interrogate.
6. Mettere il flag **Mostra il nome della postazione** per visualizzare non solo l'indirizzo IP dei computer trovati nella rete, ma anche il loro nome di dominio.

   Se una postazione non è registrata sul server DNS, viene visualizzato solo il suo indirizzo IP.

7. Mettere il flag **Correlare con la lista di postazioni dalla Base di Dati** per abilitare la sincronizzazione dei risultati della ricerca fatta da **Scanner di rete** con la lista di postazioni salvata nella Base di Dati del **Server**. Se questo flag è attivato, la lista di postazioni trovate nella rete mostrerà anche le postazioni che sono presenti nella Base di Dati del **Server**, ma non sono state rilevate da **Scanner di rete** durante la ricerca attuale, per esempio, in caso se su queste postazioni è installato il firewall che impedisce la trasmissione di pacchetti per stabilire una connessione TCP.

   Alla sincronizzazione dei risultati della ricerca fatta da **Scanner**

**di rete** con le informazioni dalla Base di Dati del **Server**, la priorità hanno le informazioni dalla Base di Dati del **Server**. Cioè se lo status di una postazione, ottenuto durante la ricerca, non corrisponde allo status registrato nella Base di Dati, verrà impostato lo status registrato nella Base di Dati.

8. Premere sul tasto **Avvia lo scanner**. Dopodiché parte la scansione di rete.
9. Durante la scansione di rete nella finestra viene caricato il catalogo (la lista gerarchica) di computer con indicazione di presenza su di essi di **Enterprise Agent**.

   Aprire elementi di catalogo, corrispondenti ai gruppi (domini). Tutti gli elementi di catalogo, corrispondenti ai gruppi e a workstation singole, vengono marcati con icone diverse, il cui significato è riportato di seguito.

**Tabelli 3-3. Vari tipi di icone**

| Icona | Descrizione |
|---|---|
| **Gruppi** | |
|  | Gruppi, che tra gli altri comprendono i computer, su cui si può installare antivirus **Dr.Web ESS**. |
|  | Altri gruppi, che comprendono i computer con il software antivirus installato o non disponibili in rete. |
| **Workstation** | |
|  | Workstation rilevata è presente nel database ed è attiva (workstation attive con il software antivirus installato). |
|  | Workstation rilevata è presente nel database di workstation remote. |
|  | Workstation rilevata non è presente nel database (sul computer non c'è il software antivirus). |
|  | Workstation rilevata non è presente nel database (workstation è connessa a un altro **Server**). |
|  | Workstation rilevata è presente nel database, non è attiva e la porta è chiusa. |

Elementi della cartella, corrispondenti a workstation con icone  o  , si possono aprire e prendere visione di contenuti dei

componenti installati.

Se si preme su icona del componente di workstation, connessa a questo **Server**, viene visualizzata la finestra delle configurazioni di questo componente.

## *Interazione con Dr.Web Enterprise Agent*

Strumento **Scanner di rete** è compreso in **Dr.Web ESS** partendo dalla versione **4.44**.



**Scanner di rete** può rilevare, se su workstation di **Agent** sono presenti solamente le versioni **4.44** e superiori, ma non è in grado di interagire con **Agent** delle versioni precedenti.

**Agent**, installato su workstation protetta, della versione e **4.44** e superiore, esegue l'elaborazione delle richieste corrispondenti di **Scanner di rete**, che arrivano su una certa porta. Di default si utilizza la porta `udp/2193`, comunque, per compatibilità con il software delle versioni precedenti è inoltre supportata la porta `udp/2372`. Quindi, le stesse porte di default si propone di richiedere e in **Scanner di rete**. **Scanner di rete** conclude se è presente o assente un **Agent** su workstation, partendo dalla possibilità di scambio delle informazioni (richiesta-risposta) via la porta sovraindicata.



Se sulla workstation è installato il blocco (per esempio, con il Firewall) di ricezione dei pacchetti su `udp/2193`, l'**Agent** non può essere rilevato e, quindi, dal punto di vista di **Scanner di rete** si considera che **Agent** su workstation non è installato.

## *Scansione rapida*

Con opzione **Scansione rapida** attiva si esegue la conseguenza successiva delle azioni:

1. Alle workstation di rete si inviano le richieste ping.
2. Solo per le workstation, che hanno risposto alle richieste di ping, viene eseguito l'interrogazione in parallelo per rilevare gli **Agent**.
3. La procedura di rilevazione della presenza di **Agent** viene eseguita a secondo le regole generali.



Richieste ping possono essere bloccate per causa delle policy di rete (per esempio, per causa delle configurazioni di Firewall).

**Per esempio**:

Se nel SO Windows Vista e superiori nelle configurazioni di rete è stata impostata la **Rete pubblica**, il SO bloccherà tutte le richieste di ping.

Durante la scansione standard non si inviano le richieste di ping, ma si richiedono consecutivamente tutte le workstation della presenza di **Agent**. Questo metodo può essere utilizzato come aggiuntivo alla scansione rapida nel caso se nella rete ci sono delle workstation su cui sono bloccate le richieste di ping.

La scansione rapida è eseguita in parallelo, la scansione standard - consecutivamente .

La velocità di operazione di **Scanner di rete** è significativamente diversa. Il tempo massimo della scansione è calcolato nel seguente modo:

- durante la scansione standard: <*N*> * <*timeout*>,
- durante la scansione rapida: <*N*>/40 + 2*<*timeout*>,

dove: <*N*> - numero workstation, <*timeout*> - valore, impostato nel campo **Time-out**.

## 3.4.2. Manager licenze

**Enterprise Server** contiene **Manager licenze**. Questo componente semplifica gestione dei file della chiave di licenza di **Server** e di **Agent.**

Per aprire la finestra di **Manager licenze**, scegliere nel menu principale del **Centro gestione** la voce **Amministrazione,** nella finestra aperta scegliere la voce del menu di gestione (pannello a sinistra) **Manager licenze**.

La finestra principale del **Manager licenze** contiene la lista gerarchica che include:

- Chiavi di server. Elementi di questa voce sono le utenze, che contengono le chiavi di licenza del **Server.** In questo caso solo una di utenze è attiva (viene utilizzata dal **Server** al momento).
- Chiavi di agent. Elementi di questa voce sono le utenze, che contengono le chiavi di licenza di **Agent**. Ogni chiave di licenza può essere destinata per più gruppi o workstation, che si visualizzano nella finestra di **Manager licenze** come elementi innestati di utenza della chiave.

***Per gestire le chiavi di licenza si utilizzano elementi della Barra degli strumenti:***

**Importo chiave** - permette di aggiungere un nuovo record su file della chiave. Per farlo, scegliere la voce corrispondente del menu a cascata:

**Aggiungi la chiave di server** - per aggiungere un nuovo file della chiave di **Server**.

**Aggiungi la chiave di agent** - per aggiungere un nuovo file della chiave di **Agent**.

**Rimuovi la chiave** - permette di eliminare utenze dei file della chiave.



Non si può eliminare utenza della chiave di **Agent**, impostato per il gruppo **Everyone**, e il record attuale attivo del file della chiave del **Server**.

 **Modifica** - per visualizzare le informazioni sulla licenza, sua attivazione (solo per **Server**) e, se è necessario, sostituzione del file della chiave (solo per **Agent**). Questa voce è attiva solo se nella finestra principale è scelta utenza del file della chiave per **Server** o **Agent**.

 **Propaga queste impostazioni verso un altro oggetto** - permette di impostare la chiave scelta su un gruppo o un workstation indicato, che si definiscono nella lista aperta. Questa voce è attiva solo se nella finestra principale è scelta l'utenza del file della chiave di **Agent**.

 **Esporta chiave** - permette di salvare la copia del file locale della chiave, scelta nella lista.

## Esempio di sostituzione di chiavi

Se si vogliono completamente sostituire (per esempio, aggiornare le licenze scadute) le chiavi di licenza dei componenti di rete antivirus (sia **Server**, sia **Agent**), eseguire le seguenti azioni nel **Manager licenze**:

1. Aggiungere una nuova chiave del Server.
2. Attivare una nuova chiave del Server.
3. Eliminare la chiave vecchia del Server.
4. Sostituire chiave di licenza di Agent per gruppo **Everyone** e, se necessario, per altri gruppi e workstation, per cui sono state impostate le chiavi di licenza personalizzate.

### 3.4.2.1. Chiavi di Dr.Web Enterprise Server

***Con il Gestore licenze si possono applicare le seguenti azioni alle chiavi di licenza di Dr.Web Enterprise Server:***

1. Visualizzare le informazioni sulla licenza.
2. Aggiungere nuove chiavi di licenza del Server.
3. Modificare validità della licenza del Server.
4. Eliminare le chiavi di licenza del Server.

## Visualizzare le informazioni sulla licenza

Per visualizzare le informazioni consuntive sulla licenza scegliere nella finestra principale del **Manager licenze** l'utenza su cui visualizzare le informazioni, e premere sul tasto **Modifica** nella barra degli strumenti. Nella barra aperta vengono visualizzate le informazioni come:

- utente di licenza,
- fornitore, da cui è stata acquistata tale licenza,
- numero di identificazione di licenza,
- data di scadenza del periodo di validità di licenza,
- se questa licenza include il supporto del plugin **Antispam**.

## Aggiungere una chiave di licenza del Server

***Per aggiungere una nuova chiave di licenza del Server:***

1. Premere sul tasto **Importo chiave** nella barra degli strumenti e nella lista a cascata scegliere la voce **Aggiungi la chiave di server**.
2. Nella barra aperta premere sul tasto **Sfogliare** e scegliere un file con la chiave di licenza del **Server**.
3. Premere sul tasto **Salva**.

Si possono impostare più utenze con i file della chiave. In questo caso solo una licenza del **Server** sarà attiva.

Se si sostituisce il file della chiave del **Server** (durante l'attivazione di file della chiave nuovo), i parametri `ID1` del **Server** nei file della chiave nuovo e quello precedente saranno diversi, mentre l'orario del **Server**, le configurazioni di comunicazioni intraserver e statistiche dei processi del **Server** saranno perse.

Per salvare l'orario del **Server** si deve eseguire la sua esportazione prima di sostituire la chiave di licenza e l'importazione - dopo la sostituzione.

## Modifica di validità di licenza del Server

Se ci sono più utenze con i file della chiave, solo una delle licenze del **Server** è attiva (utilizzata dal **Server** al momento).

***Per modificare la licenza attiva del Server:***

1. Scegliere l'utenza con la licenza da installare sul **Server** e premere sul tasto **Modificare** nella barra degli strumenti.
2. Nella barra aperta premere sul tasto **Attivare**.
3. Dopo l'attivazione di una chiave del server nuova, per continuare con l'operazione riavviare il **Server**.

## Eliminazione di chiave della licenza del Server

Non si può eliminare l'utenza corrente attiva del file della chiave del **Server**.

***Per eliminare la chiave di licenza del Server a disposizione:***

1. Scegliere nel menu principale del **Gestore licenze** la chiave da eliminare e premere sul tasto **Rimuovi la chiave** nella barra degli strumenti.
2. Nella finestra di dialogo confermare l'eliminazione della chiave.

### 3.4.2.2. Chiavi di Dr.Web Enterprise Agent

***Con il Gestore licenze si possono eseguire le seguenti azioni con le chiavi di licenza di Dr.Web Enterprise Agent:***

1. Visualizzare le informazioni sulla licenza.
2. Aggiungere nuove chiavi di licenza del Server.
3. Sostituire chiavi di licenza di Agent con chiavi nuove.
4. Sostituire chiavi di licenza di Agent con chiavi che già fanno parte di rete antivirus.
5. Eliminare le chiavi di licenza del Server.

## Visualizzare le informazioni sulla licenza

Per visualizzare le informazioni consuntive sulla licenza scegliere nella finestra principale del **Manager licenze** l'utenza su cui visualizzare le informazioni, e premere sul tasto **Modifica** nella barra degli strumenti. Nella barra aperta vengono visualizzate le informazioni come:

- utente di licenza,
- fornitore, da cui è stata acquistata tale licenza,
- numero di identificazione di licenza,
- data di scadenza del periodo di validità di licenza,
- se questa licenza include il plugin **Antispam,**
- quali componenti antivirus sono compresi in questa licenza.

## Aggiungere una chiave di licenza di Agent



Si possono impostare più utenze con i file della chiave di **Agent**.

***Per aggiungere una nuova chiave di licenza del Agent:***

1. Premere sul tasto  **Importo chiave** nella barra degli strumenti e nella lista a cascata scegliere la voce  **Aggiungi la chiave di agent**.
2. Nella barra aperta premere sul tasto **Sfogliare** e scegliere un file con la chiave di licenza di **Agent**.
3. Premere sul tasto **Salva**.

## Sostituire chiave di licenza di Agent con una chiave nuova

***Per sostituire una chiave di licenza di Agent attuale con una chiave nuova:***

1. Scegliere nella finestra principale del **Manager licenze** l'oggetto (workstation o gruppo), per cui è destinata la chiave da sostituire e premere sul tasto  **Modifica** nella barra degli strumenti.
2. Nella barra aperta premere sul tasto **Sfogliare** e scegliere il file con la chiave di licenza di **Agent**.
3. Premere sul tasto **Salva**.
4. Se la lista dei componenti che si possono installare secondo la licenza su workstation della chiave nuova è diversa dalla lista della chiave precedente, viene visualizzata la richiesta di impostare le configurazioni secondo la lista dei componenti della chiave nuova.

   Nella lista di oggetti proposta sono indicati workstation e gruppi, le cui liste della chiave precedente e della chiave importata sono

diversi, e la lista di differenze (quali componenti sono assenti o sono aggiunti alla chiave nuova). Mettere i flag su oggetti, per cui saranno impostati le configurazioni nuove delle liste di componenti installati. Le configurazioni di altri oggetti (sui cui i flag non sono posti) rimangono come prima della sostituzione della chiave.

## Sostituire chiave di licenza di Agent con una chiave già esistente

***Per sostituire una chiave di licenza di Agent attuale con una chiave che già fa parte di rete antivirus:***

1. Scegliere nella finestra principale del **Manager licenze** la chiave da destinare per oggetto (workstation o gruppo) e premere sul tasto **Propaga queste impostazioni verso un altro oggetto** nella barra degli strumenti.
2. Nella finestra aperta scegliere dalla lista workstation o gruppo richiesti (questo gruppo deve contenere workstation). Per scegliere uno o più oggetti si deve premere con il tasto sinistro del mouse su di essi, e lo stesso per togliere la scelta.
3. Premere sul tasto **Salva**.

> Se per workstation o gruppo è già impostata una chiave nelle configurazioni personalizzate, per impostare una nuova chiave, che è nella lista della finestra principale del **Manager licenze**, è sufficiente spostare questo gruppo o workstation con il mouse (drag and drop) su utenza della chiave (in questo caso può esserci un minore ritardo in aggiornamento di lista della finestra principale).

4. Se la lista dei componenti che si possono installare secondo la licenza su workstation della chiave nuova è diversa dalla lista della chiave precedente, viene visualizzata la richiesta di impostare le configurazioni secondo la lista dei componenti della chiave nuova.

   Nella lista di oggetti proposta sono indicati workstation e gruppi, le cui liste della chiave precedente e della chiave importata sono

diversi, e la lista di differenze (quali componenti sono assenti o sono aggiunti alla chiave nuova). Mettere i flag su oggetti, per cui saranno impostati le configurazioni nuove delle liste di componenti installati. Le configurazioni di altri oggetti (sui cui i flag non sono posti) rimangono come prima della sostituzione della chiave.

## Eliminazione chiave di licenza di Agent



Non si può eliminare l'utenza di chiave di **Agent**, destinato per gruppo **Everyone**.

***Per eliminare una chiave di licenza di Agent a disposizione:***

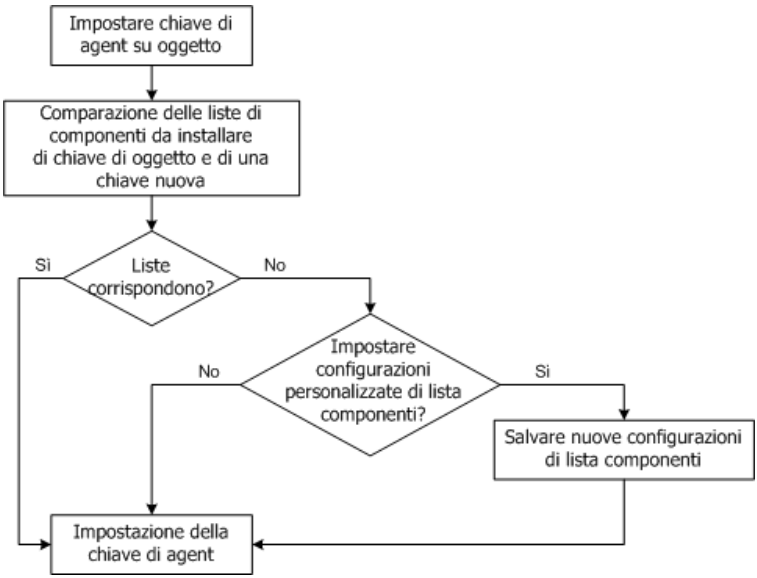
1. Scegliere nel menu principale del **Manager licenze** la chiave da eliminare, o l'oggetto (workstation o gruppo), per cui è destinata tale chiave, e premere sul tasto  Rimuovi la chiave nella barra degli strumenti.
2. Nella finestra di dialogo confermare l'eliminazione della chiave.
3. Se per oggetto, da cui viene eliminata la chiave, sono state impostate delle configurazioni personalizzate della lista dei componenti installati, viene visualizzata una richiesta di eliminare le configurazioni personalizzate.

   Nella lista di oggetti proposta sono indicati workstation e gruppi con le configurazioni personalizzate. Mettere i flag su oggetti, per cui viene impostata l'ereditarietà delle configurazioni dal gruppo padre. Sul resto di oggetti saranno conservate le configurazioni personalizzate delle liste dei componenti installati come prima di eliminazione della chiave.

# Modifica della lista dei componenti installati

## *Sostituire o aggiungere di una nuova chiave di licenza*

Se le liste di componenti installati nella chiave nuova e quella precedente sono diverse, le configurazioni delle liste dei componenti installati di oggetto si possono sostituire con delle nuove o si possono conservare (v. Sostituire chiave di licenza di Agent).


Impostare chiave di agent su oggetto
Comparazione delle liste di componenti da installare di chiave di oggetto e di una chiave nuova
Liste corrispondono?
Sì
No
Impostare configurazioni personalizzate di lista componenti?
No
Sì
Salvare nuove configurazioni di lista componenti
Impostazione della chiave di agent

**Procedura di sostituzione o di aggiunta di una nuova chiave di Agent**

### *Se si impostano delle configurazioni nuove:*

1. Se nella chiave nuova ci sono componenti che non c'erano nella chiave precedente, per tali componenti nella lista **Componenti da installare** si imposta il valore **può** (v. Configurazione workstation). Di seguito l'utente avrà la possibilità di installare questi componenti su workstation, che vengono registrate con la nuova chiave.

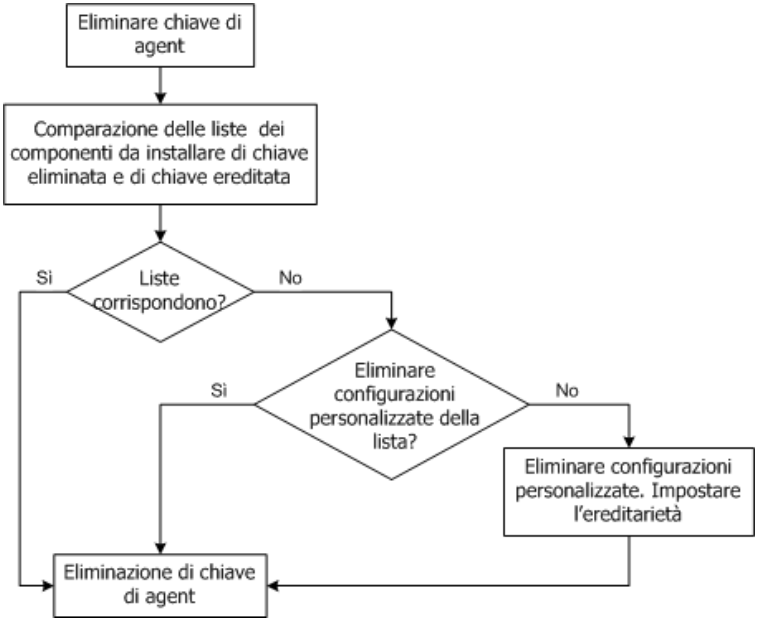
2. Se nella nuova chiave non sono inclusi i componenti, che erano inclusi nella chiave precedente, per tali componenti nella lista **Componenti da installare** sarà impostato il valore **non può**, ed essi saranno eliminati da workstation che vengono registrate con la nuova chiave.
3. Per tutti gli altri componenti, compresi nella chiave precedente e nella chiave nuova, le configurazioni della pagina **Componenti da installare** saranno salvati come prima della sostituzione della chiave.

***Se le configurazioni si conservano:***

Nella pagina **Componenti da installare** rimangono configurazioni precedenti a eliminazione della chiave.

## *Eliminare la chiave di licenza*

Le configurazioni di liste di componenti installati si possono ereditare dal gruppo padre oppure conservarsi (v. Eliminare chiave di licenza di Agent).




**Procedura di eliminazione della chiave di licenza di Agent**

***Se le configurazioni si ereditano:***

Nella pagina **Componenti da installare** saranno eliminate tutte le configurazioni personalizzate e sarà impostata l'ereditarietà delle configurazioni del gruppo padre.

***Se le configurazioni si conservano:***

Nella pagina **Componenti da installare** rimangono configurazioni precedenti a eliminazione della chiave.

# 3.5. Schema interazione componenti rete antivirus

In immagine 3-3 è rappresentato lo schema generale di una parte di rete antivirus.

Tale schema rappresenta una rete antivirus, di cui fa parte solo un **Server**. Nelle grosse società è preferibile ogranizzare una rete antivirus con più **Server** per distribuire il carico tra di essi.

In questo esempio la rete antivirus è implementata nel quadro di un LAN, però per l'installazione e l'operazione di **ESS** e pacchetti antivirus non è necessario che i computer si trovino nel quadro di un LAN, è sufficiente accesso Internet.

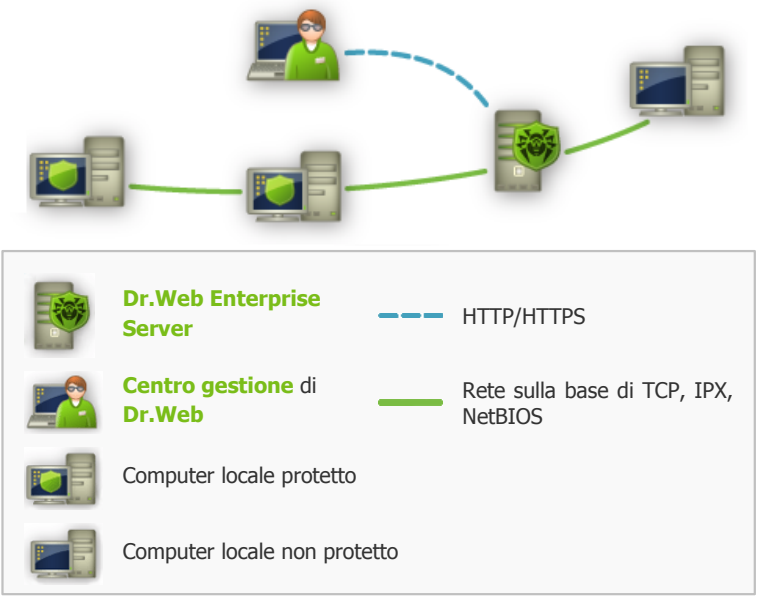



**Immagine 3-3. Struttura di rete antivirus**

***All'avvio di Dr.Web Enterprise Server si eseguiscono le azioni successive:***

1. Carico dei file di **Enterprise Server** dalla cartella `bin`.
2. Carico di **Schedulatore processi** del **Server**.
3. Carico della cartella di installazione centralizzata e di cartella di aggiornamenti, inizializzazione del sistema di informazione (sistema di avvisi).
4. Controllo integrità del database del **Server**.

5. Esecuzione dei processi di **Schedulatore processi** del **Server.**
6. Attesa delle informazioni da **Enterprise Agent** e dei comandi dai **Centri gestione**.

Tutto il flusso dei comandi, dei dati e delle informazioni statistiche nella rete antivirus necessariamente passa tra **Enterprise Server**. Il **Centro gestione** inoltre scambia le informazioni solamente con il **Server**; le modifiche nelle configurazioni della rete antivirus e la trasmissione di comandi a **Enterprise Agent** sono eseguite dal **Server** sulla base dei comandi del **Centro gestione**.

In questo modo, la struttura logica della parte di rete antivirus è come presentata in immagine 3-4.

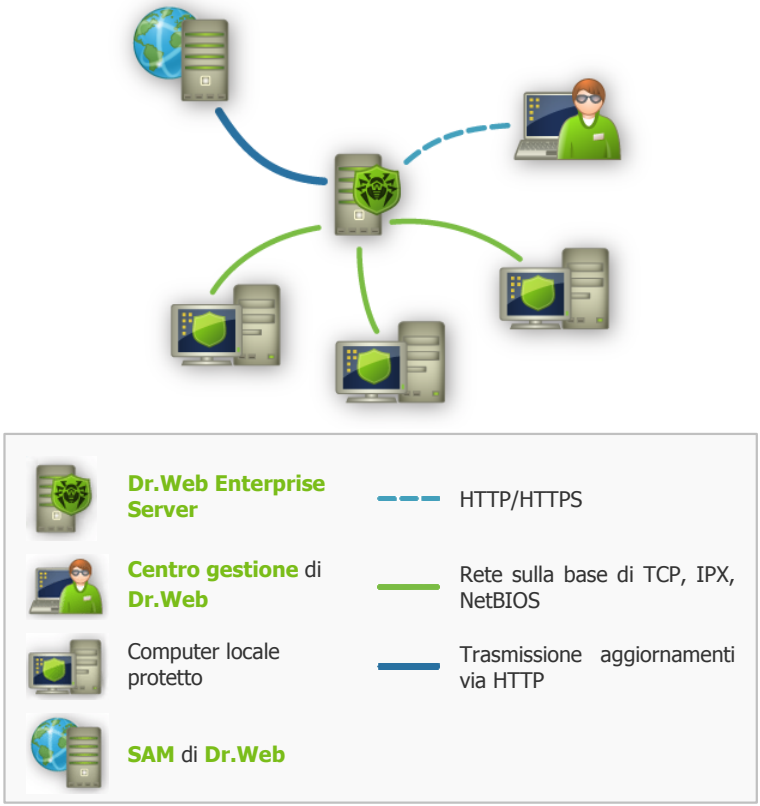



**Immagine 3-4. Struttura logica di rete antivirus**

Tra **Server** e workstation (una linea continua sottile in immagine 3-4) via uno dei protocolli di rete supportati (TCP/IP, IPX o NetBIOS) si trasmettono:

- richieste di **Agent** per ottenere un orario centralizzato e orario centralizzato di tale workstation,
- configurazioni di **Agent** e del pacchetto antivirus,
- richieste dei processi ordinari da eseguire (scansione, aggiornamento dei database dei virus ecc),
- file dei pacchetti antivirus - alla ricezione di **Agent** del processo

di loro installazione,

- aggiornamenti del software e dei database dei virus - durante l'esecuzione del processo di aggiornamento,
- avvisi di **Agent** della configurazione di workstation,
- statistiche di operazione di **Agent** e dei pacchetti antivirus per includerle nel log centralizzato,
- avvisi degli eventi dei virus e di altri eventi da registrare.

Il volume di traffico tra workstation e **Enterprise Server**, secondo le configurazioni di workstation e il loro numero, può essere abbastanza significativo. Per questo la rete antivirus di **Dr.Web ESS** prevede la possibilità di comprimere il traffico. Per descrizione di utilizzo di tale modalità facoltativa v. sotto, Utilizzo codifica e compressione traffico.

Si può codificare il traffico tra **Enterprise Server** e workstation. Questo permette di evitare divulgazione delle informazioni, trasmesse via il canale descritto, nonché sostituzione del software, caricato su workstation. Di default questa possibilità è attiva. Per descrizione di utilizzo di tale modalità v. sotto, Utilizzo codifica e compressione traffico.

Dal server web di aggiornamenti a **Enterprise Server** (linea continua spessa in immagine 3-4) si trasmettono, con utilizzo del protocollo HTTP, i file, necessari per replicare le cartelle centralizzate di installazione e di aggiornamento, e le informazioni di servizio sullo stato di tale processo. L'integrità delle informazioni trasmesse (file del software di **Dr.Web ESS** e pacchetti antivirus) è assicurata dall'utilizzo del metodo checksum: il file danneggiato o sostituito durante la trasmissione non sarà accettato dal **Enterprise Server**.

Tra il **Enterprise Server** e il **Centro gestione** (linea discontinua in immagine 3-4) si passano le informazioni sulla configurazione del **Enterprise Server** (comprese le informazioni sulla topologia di rete) e le configurazioni di workstation. Queste informazioni si visualizzano nel **Centro gestione**, e, se l'utente (amministratore di rete antivirus) completamente modifica qualche configurazione, se ne trasmettono le informazioni su modifiche introdotte al **Enterprise Server**.

Si stabilisce connessione del **Centro gestione** al **Enterprise Server** scelto, che viene eseguita solamente dopo l'autenticazione di

amministratore di rete antivirus, inserendo il nome di registrazione e la chiave su tale **Enterprise Server**.

# Capitolo 4. Inizio lavoro. Informazioni generali

## 4.1. Creazione rete antivirus semplice



Prima di iniziare di utilizzare il software antivirus si consiglia di modificare le impostazioni della cartella di backup di dati critici del **Server** (v. Impostazione orario di Dr.Web Enterprise Server). Sarebbe meglio locare questa cartella su altro disco locale per diminuire i rischi di perdita contemporanea dei file di software del **Server** e della copia di riserva.

### *Connessione via Centro gestione Dr.Web*

Di default **Enterprise Server** si avvia automaticamente dopo l'installazione e dopo ogni riavvio del sistema (v. anche Dr.Web Enterprise Server).

Per installare il **Server** e il software antivirus su workstation si deve collegarsi al **Server** via **Centro gestione Dr.Web**.

Su ogni computer, che ha accesso di rete a **Enterprise Server**, **Centro gestione** è disponibile all'indirizzo:

`http://`*<Indirizzo_Server>*`:9080`

o

`https://`*<Indirizzo_Server>*`:9081`

dove come *<Indirizzo_Server>* indicare indirizzo IP o nome di dominio del computer, su cui è installato **Enterprise Server**.

Nella finestra di dialogo di richiesta di autorizzazione inserire il nome e la password dell'amministratore (nome amministratore predefinito –

**admin**, password – password, che è stata impostata all'installazione del **Server**, v. Installazione di Dr.Web Enterprise Server).

Alla connessione avvenuta con successo al **Server** si apre la finestra principale del **Centro gestione**. In questa finestra viene visualizzata l'informazione su rete antivirus, gestita da questo **Server** (per descrizione dettagliata v. Centro gestione di Dr.Web).

## *Gestione rete antivirus*

Con **Centro gestione** si possono gestire **Server** e rete antivirus:

- creare workstation antivirus (v. Installazione di Dr.Web Enterprise Agent via Centro gestione Dr.Web),
- confermare workstation,
- modificare, configurare e eliminare workstation antivirus (v. Gestione workstation),
- configurare e modificare le connessioni con **Enterprise Server** vicini (v. Particolarità di rete con più Server),
- visualizzare i log di eventi di questo **Server** e di **Server** vicini ed altri dati.

Strumenti principali di gestione sono concentrati nel menu principale, nel menu di gestione e nella barra degli strumenti (v. Centro gestione Dr.Web).

## *Connessione a Dr.Web Enterprise Agent*

Dopo l'installazione di **Agent** su workstation via pacchetto di installazione, **Agent** cerca di connettersi a **Enterprise Server**.

Nelle impostazioni di **Enterprise Server** di default l'amministratore deve manualmente confermare le workstation nuove per registrarle sul **Server** (per più informazioni su politica di connessione di workstation nuove v. Politica di connessione di workstation). In questo caso le workstation nuove non vengono connesse automaticamente, ma vengono messe da **Server** nella lista di workstation non confermate.

***Per consentire la connessione di una workstation nuova a Dr.Web Enterprise Server:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**.
2. Nella finestra aperta scegliere la voce del menu di gestione **Postazioni non confermate**.
3. Si apre la finestra con la lista di workstation, su cui è installato **Agent,** ma cui accesso non è ancora confermato.
4. Scegliere workstation nella lista (mettere il flag accanto), dopodiché nella barra degli strumenti scegliere la voce **Consenti l'accesso e designa come primario il gruppo**, per confermare l'accesso di questa workstation. Verrà proposto di scegliere il gruppo primario per la workstation.

   Per più informazioni su gruppi primari v. Ereditarietà di elementi di configurazione di workstation. Gruppi primari.

5. Workstation viene connessa al **Server**, e l'immaggine di icona di workstation nella rete antivirus viene cambiata.

   Workstation viene aggiunta ai gruppi predefiniti di workstation **Everyone**, **Online**, ed ai gruppi, che corrispondono al protocollo di connessione, alla famiglia del sistema operativo e al sistema operativo concreto.

### *Installazione del software antivirus*

Installazione di componenti di pacchetto antivirus su workstation procede senza intervento dell'amministratore.



Su workstation vengono installati i componenti del pacchetto antivirus, indicati nelle impostazioni del gruppo primario di workstation (per più informazioni v. Contenuti pacchetto antivirus).

Per completare l'installazione di alcuni componenti di workstation antivirus potrebbe essere richiesto il riavvio del computer. In questo caso sullo sfondo di icona di **Enterprise Agent** nella **Barra degli applicazioni** appare il punto esclamativo nel triangolo giallo (v. anche Dr.Web Enterprise Agent).

# 4.2. Configurazione connessioni di rete

## Informazioni generali

A **Enterprise Server** si connettono i seguenti client:

- **Enterprise Agent**,
- **Installazione di rete** di **Enterprise Agent**,
- altri **Enterprise Server**.

Connessione è sempre stabilita su iniziativa del client.

Sono disponibili i seguenti modi di connessione di client al **Server**:

1. Tramite connessione diretta.

   Questo approccio ha tanti vantaggi, ma non è sempre preferibile (ci sono perfino delle situazioni, quando non si deve utilizzarlo).

2. Tramite Servizio rilevazione Server.

Di default (se non è impostato altrimenti) i client utilizzano proprio questo **Servizio**.

Questo approccio è da utilizzare se è necessaria la reconfigurazione di tutto il sistema, in particolare, se si deve trasferire **Enterprise Server** su altro computer o cambiare l'indirizzo IP del computer su cui è installato il **Server**.

Quando si configura la rete antivirus **ESS** per l'utilizzo delle connessioni dirette, **Servizio rilevazione Server** può essere disattivato. Per farlo, nella descrizione di trasporti (**Amministrazione** → **Configurazione Dr.Web Enterprise Server** → scheda **Trasporto**) si deve lasciare vuoto il campo Indirizzo del cluster.

## Connessioni dirette

### *Configurazione di Dr.Web Enterprise Server*

Nelle impostazioni del **Server** si deve indicare, del quale indirizzo (v. Allegato E. Specificare indirizzo di rete) essere "in ascolto" per ricevere le connessioni TCP in arrivo.

Questo parametro viene indicato nelle impostazioni del **Server** **Amministrazione** → **Configurazione Dr.Web Enterprise Server** → scheda **Trasporto** → campo **Indirizzo**.

Di default "ascolto" del **Server** si impostano:

- `tcp/0.0.0.0:2371` - supportato per compatibilità inversa; in particolare, per evitare i problemi con il passaggio dalle versioni **4.XX**, dove si utilizza la porta `2371`.
- `tcp/0.0.0.0:2193` - nel caso di utilizzo della porta `2193`, registrata a **Dr.Web Enterprise Security Suite** in IANA.

Sigla `0.0.0.0` significa "tutte le interfacce di rete" per il computer, su cui è installato il **Server**.

Per il funzionamento corretto di tutto il sistema **ESS** è sufficiente, che il **Server** sia in ascolto di almeno una porta TCP, che deve essere conosciuta da tutti i client.

## *Configurazione di Dr.Web Enterprise Agent*

Durante l'installazione di **Agent** l'indirizzo del **Server** (indirizzo IP o nome del computer di rete, dove è avviato **Enterprise Server**) può essere esplicitamente indicato nei parametri di installazione:
`drwinst` <*Indirizzo_Server*>

All'installazione di **Agent** si consiglia di utilizzare il nome del **Server**, registrato precedentemente nel servizio DNS. Questo semplifica il processo di configurazione di rete antivirus, legato alla procedura di reinstallazione di **Enterprise Server** su altro computer.

Di default il comando `drwinst`, avviato senza parametri, scansiona la rete per la presenza di **Enterprise Server** e cerca di installare **Agent** dal primo **Server**, rilevato in rete (modalità *Multicasting* con utilizzo di Servizio rilevazione Server).

In questo modo, l'indirizzo di **Enterprise Server** diventa conosciuto da **Agent** all'installazione.

Di seguito l'indirizzo del **Server** può essere modificato manualmente nelle impostazioni di **Agent**. Visualizzazione e modifica delle impostazioni di connessione a **Enterprise Server** viene eseguito via la voce del menu contestuale dell'icona di **Agent** **Impostazioni** → **Connessione.**

## Servizio rilevazione di Dr.Web Enterprise Server

Con questo schema il client non conosce inizialmente l'indirizzo del **Server**. A ogni connessione si effettua la ricerca del **Server** nella rete. Per farlo, il client invia nella rete una richiesta broadcast e aspetta la risposta dal **Server** che ne indichi l'indirizzo. Dopo aver ricevuto la risposta, il client stabilisce la connessione al **Server**.

Per farlo, **Server** deve rimanere "in ascolto" di tali richieste sulla rete.

Ci sono alcune varianti di configurazione di tale schema. L'importante è che il metodo di ricerca del **Server**, impostato per i client, corrisponda alle impostazioni della parte relativa del **Server**.

In **Enterprise Security Suite** di default viene utilizzata la modalità *Multicast over UDP*:

1. **Server** viene registrato nel gruppo multicast con l'indirizzo `231.0.0.1`.
2. **Agent**, alla ricerca del **Server**, inviano in rete le richieste multicast all'indirizzo di gruppo `231.0.0.1`.

Di default per "ascolto" del **Server** si impostano (come nelle connessioni dirette):

- `udp/231.0.0.1:2371`
- `udp/231.0.0.1:2193`

Questo paramentro viene configurato nelle impostazioni del **Server** **Amministrazione** → **Configurazione Dr.Web Enterprise Server** → scheda **Trasporto** → campo **Indirizzo del cluster**.

## Configurazione di Firewall

Per interazione di componenti di rete antivirus è necessario, che tutte le porte e le interfacce utilizzate siano aperte su tutti i computer, che fanno parte di rete antivirus.

Durante l'installazione del **Server** l'installazione propone di aggiungere automaticamente le esclusioni nelle impostazioni di Firewall del sistema operativo Windows (oltre il sistema operativo Windows 2000). Per farlo, mettere il flag **Aggiungere alle esclusioni di Firewall porte e interfacce del server**.

Se si utilizza il Firewall, oltre il Firewall incorporato del sistema operativo Windows, l'amministratore di rete antivirus deve eseguire manualmente le impostazioni corrispondenti.

# Capitolo 5. Amministratori di rete antivirus

Si consiglia di nominare l'amministratore di rete antivirus uno specialista affidabile, qualificato, che abbia un'esperienza di amministrazione di rete locale e sia competente nella protezione antivirus. Tale specialista deve avere accesso completo alle cartelle di installazione di **Enterprise Server**. Secondo la politica di sicurezza della società e della composizione del personale, l'amministratore della rete antivirus deve avere i diritti dell'amministratore della rete locale o lavorare nel contatto stretto con tale persona.



All'Amministratore di rete antivirus per la gestione corrente di rete antivirus non servono i diritti dell'amministratore su workstation, che fanno parte di tale rete antivirus. Comunque installazione remota e deinstallazione del software di **Agent** è disponibile solamente nella rete locale e non richiede i diritti dell'amministratore di tale rete, e debugging di **Enterprise Server** — accesso completo alla cartella della sua installazione.

## 5.1. Autenticazione di amministratori

***Autenticazione di amministratore per connettersi a Enterprise Server può essere fatta nei seguenti modi:***

1. Salvando i dati di amministratore nel database del **Server**.
2. Con Active Directory (nelle versioni del **Server** per i SO Windows).
3. Utilizzando protocollo LDAP.
4. Utilizzando protocollo RADIUS.

***Modi di autenticazione vengono utilizzati consecutivamente secondo i seguenti principi:***

1. L'ordine di utilizzo dei metodi di autenticazione dipende dall'ordine in cui essi si susseguono nelle impostazioni definite tramite il **Centro Gestione**.
2. Prima si esegue il tentativo di autenticare l'amministratore dal database del **Server**.
3. Come seconda di default viene utilizzata l'autenticazione via LDAP, terza - tramite ActiveDirectory, quarta - tramite RADIUS.
4. Nelle impostazioini del **Server** la conseguenza dei modi di autenticazione via LDAP, Active Directory e RADIUS può essere modificata, ma all'inizio si esegue sempre il tentativo di autenticare l'amministratore dal database.
5. Modi di autenticazione via LDAP, Active Directory e RADIUS di default sono sempre disattivati.

***Per modificare l'ordine di utilizzo dei metodi di autorizzazione:***

1. Scegliere la voce **Amministrazione** nel menu principale del **Centro Gestione**.
2. Nel menu di gestione scegliere la sezione **Autorizzazione**.
3. Nella finestra aperta si presenta la lista dei tipi di autorizzazione disposti secondo l'ordine in cui essi vengono utilizzati. Per modificare quest'ordine, premere sulla freccia a sinistra del nome del tipo di autorizzazione. Le voci con i nomi del tipo di autorizzazione si scambiano i posti.

## Autenticazione di amministratori dal Server database

Il modo di autenticazione che salva i dati di amministratori nel database del **Server** viene utilizzato di default.

***Per gestire la lista di amministratori:***

1. Scegliere la voce **Amministrazione** nel menu principale del **Centro Gestione**.

2. Nel menu di gestione scegliere la sezione **Amministratori**. Si apre la lista di tutti gli amministratori, registrati nel database.

   Per più informazioni v. Gestione utenze amministratori.

## Autenticazione con utilizzo di Active Directory

***Per attivare autenticazione via Active Directory:***

1. Scegliere la voce **Amministrazione** nel menu principale del **Centro Gestione**.
2. Nel menu di gestione scegliere la sezione **Autorizzazione**.
3. Nella finestra aperta entrare nella sezione **Microsoft Active Directory**.
4. Mettere il flag **Usa l'autorizzazione Microsoft Active Directory**.
5. Premere **Salva**.

Durante l'autenticazione di amministratori via Active Directory nel **Centro Gestione** si imposta solo il permesso di utilizzo di tale metodo di autenticazione.

La modifica delle opzioni di amministratori di Active Directory viene eseguita manualmente sul server Active Directory.

***Per modificare amministratori di Active Directory:***



Le seguenti operazioni si eseguono su un computer che ha attrezzatura per amministrare Active Directory.

1. Per poter modificare i parametri di amministratori si deve modificare lo schema di Active Directory:
   a) Per modificare lo schema di Active Directory, avviare utilità `drwschema-modify.exe` (fa parte della distribuzione di **Enterprise Server**).
   Per modificare lo schema di Active Directory potrebbe occorrere un certo tempo. A seconda della configurazione del dominio, ci vogliono oltre 5 minuti per sincronizzare e applicare lo schema modificato.

b) Per registrare l'attrezzatura Active Directory Schema (lo Schema di Active Directory), eseguire con i permessi di amministratore il comando `regsvr32 schmmgmt.dll`, dopodiché avviare `mmc` e aggiungere l'attrezzatura **Active Directory Schema**.

c) Utilizzando l'attrezzatura Active Directory Schema aggiungere alla classe **User** e (se necessario) alla classe **Group** la classe ausiliaria **DrWebEnterpriseUser**.



Se l'applicazione di schema modificato non si è completata ancora, la classe **DrWebEnterpriseUser** può essere non trovato. In questo caso aspettare per un tempo e ripetere il tentativo secondo il punto **c)**.

d) Con i permessi di amministratore avviare il file `drweb-esuite-aduac-600-xxxxxxxxx-windows-nt-xYY.msi` (fa parte della distribuzione di **Dr.Web Enterprise Security Suite 6.0.4**) e aspettare il compimento dell'installazione.

2. Interfaccia grafica per modificare attributi è disponibile nel pannello di controllo **Active Directory Users and Computers** → sezione **Users** → nella finestra di modifica delle opzioni dell'utente scelto **Administrator Properties** → nella scheda **Dr.Web Authentication**.
3. Si possono modificare i seguenti parametri (i valore di ogni attributo può essere **yes**, **no** o **not set**):

   - **User is administrator** - indica che utente è un amministratore con i diritti completi.
   - **User is read-only administrator** - indica che utente è un amministratore con i diritti di sola lettura.

     Se il valore **yes** è impostato solo per parametro **User is administrator**, utente è amministratore con i diritti completi.

     Se il valore **yes** è impostato per parametri **User is administrator** e **User is read-only administrator** contemporaneamente, utente è amministratore con i diritti di sola lettura.

- **Inherit permissions from groups** - parametro, che consente l'ereditarietà di valori di altri parametri da gruppi utenti. Se qualche parametro (o più parametri) hanno valore **not set** e per **Inherit permissions from groups** è impostato valore **yes**, i valori di parametri non impostati vengono ereditati dai gruppi, di cui fa parte questo utente.



Per algoritmi di operazione e analisi di requisiti all'autorizzazione v. Allegato O.

## Autenticazione con utilizzo di LDAP

***Per attivare autenticazione via LDAP:***

1. Scegliere la voce **Amministrazione** nel menu principale del **Centro Gestione**.
2. Nel menu di gestione scegliere la sezione **Autorizzazione**.
3. Nella finestra aperta entrare nella sezione **Autorizzazione LDAP.**
4. Mettere il flag **Usa autorizzazione LDAP**.
5. Premere **Salva**.

Configurazione di autorizzazione con utilizzo del protocollo LDAP è disponibile su ogni server LDAP. Inoltre con utilizzo dello stesso meccanismo si può configurare il **Server** sotto SO della famiglia UNIX per autorizzazione in Active Directory su controller di dominio.



Impostazioni di autorizzazione LDAP vengono salvati nel file di configurazione `auth-ldap.xml`.

Per descrizione di attributi xml principali di autorizzazione v Allegato O.

A differenza da Active Directory, si può impostare il meccanismo su qualsiasi schema LDAP. Di default viene eseguito il tentativo di utilizzare gli attributi **Dr.Web Enterprise Security Suite**, come definiti per Active Directory.

***Processo di autorizzazione LDAP è seguente:***

1. Indirizzo del server LDAP viene impostato via il **Centro Gestione** o nel file di configurazione xml.
2. Per il nome utente impostato si eseguono le seguenti azioni:
   - Si esegue la traslazione del nome in DN (Distinguished Name) con utilizzo di maschere simili a DOS (utilizzando il carattere *), se le regole sono impostate.
   - Si esegue la traslazione del nome in DN con utilizzo delle espressioni regolari, se le regole sono impostate.
   - Si utilizza lo script custom di traslazione dei nomi in DN, se specificato nelle impostazioni.
   - Se non è adatta nessuna regola di conversione, nome utilizzato viene utilizzato così com'è.



Il formato di impostazione nome utente non è in nessun modo definito o fissato - può essere lo stesso utilizzato dalla società, cioè la modifica dello schema LDAP coattiva non è richiesta. La conversione secondo tale schema viene eseguita, utilizzando le regole di translazione nomi in LDAP DN.

3. Dopo la traslazione, come con Active Directory, con DN ottenuto e password inserita si esegue il tentativo di registrare questo utente su server LDAP indicato.
4. Dopodiché, così come in Active Directory, vengono letti attributi dell'oggetto LDAP per DN ottenuto. Attributi e loro eventuali valori possono essere redifiniti nel file di configurazione.
5. Nel caso in cui valori di alcuni attributi dell'amministratore non sono definiti, se è impostata l'ereditarietà (nel file di configurazione), la ricerca di attributi richiesti per i gruppi, di cui fa parte l'utente, è eseguita come con Active Directory.

# 5.2. Tipi amministratori



In questa sezione sono presenti informazioni su amministratori, i cui dati di credenziali vengono registrati nel database di **Enterprise Server**.

***Utenze di amministratori di rete antivirus si suddividono in 4 gruppi:***

- amministratori con i diritti completi,
- amministratori con i diritti di sola lettura,
- amministratori di gruppi con i diritti completi,
- amministratori di gruppi con i diritti di sola lettura.

## *Amministratori con i diritti completi*

Amministratori con i diritti completi hanno i diritti esclusivi della gestione di **Enterprise Server** e della rete in generale. Possono visualizzare e modificare configurazione della rete antivirus, nonché creare nuove utenze amministrative. Amministratore con tali diritti ha i diritti completi di gestione del software antivirus su workstation. In questo caso può limitare, fino al divieto completo, l'intervento dell'utente di workstation nella gestione del software antivirus (v. Configurazione diritti utenti).

Amministratore con i diritti completi può visualizzare e modificare la lista di utenze amministratori esistenti.

## *Amministratori con i diritti di sola lettura*

Amministratori con i diritti di sola lettura possono solamente visualizzare impostazioni di rete generali ed elementi singoli, ma non modificarli.

### *Amministratori di gruppi con i diritti completi*

Amministratori di gruppi hanno accesso a tutti i gruppi di sistema e a gruppi utenti, la cui gestione gli è consentita (compresi innestati). Si possono creare tali credenziali solo per gruppi utente (v. Gruppi di sistema e di utente). Per tale amministratore nell'albero gerarchico saranno visualizzati solamente i gruppi, a cui ha accesso.

Amministratori di gruppi non possono visualizzare la lista di credenziali di amministratori esistenti.

### *Amministratori di gruppi con i diritti di sola lettura*

Amministratori di gruppi possono avere sia i diritti completi di modifica dei gruppi che gli sono consentiti, sia i diritti di sola lettura.

### *Amministratori predefiniti*

Dopo installazione del **Server** viene automaticamente creata utenza **admin** - amministratore con i diritti completi. La password per accedere con questa utenza viene impostato durante l'installazione del **Server** (passo 15 di procedura di installazione).

## 5.3. Gestione utenze amministratori



In questa sezione sono presenti informazioni su gestione amministratori, i cui dati di utenze sono registrati nel database di **Enterprise Server**.

***Amministratori con i diritti completi possono:***

- Creare utenze di amministratori nuove ed eliminare quelle già esistenti.

- Modificare le impostazioni di tutti gli amministratori di rete antivirus.

***Amministratori dei gruppi e amministratori con i diritti di sola lettura possono:***

- Modificare una parte delle impostazioni solo della sua utenza.

## 5.3.1. Creazione e eliminazione amministratori

### Aggiungere amministratore

***Per aggiungere una nuova utenza amministratore:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Amministratori**.
2. Premere nella barra degli strumenti l'icona **Crea un account**.
3. Si apre la finestra impostazioni di utenza creata. Impostare i seguenti parametri:
   - Nel campo **Nome di registrazione** indicare il login dell'amministratore da utilizzare per accedere al **Centro gestione**.
   - Nei campi **Password** e **Password ripetuta** impostare la password per accedere al **Server**.

   Nella password amministratore non si possono utilizzare i caratteri nazionali.

   - Mettere il flag **Sola lettura** per limitare i diritti di accesso.
   - Nei campi **Cognome**, **Nome** e **Patronimico** si possono indicare i dati personali dell'amministratore.
   - Nella lista a cascata **Lingua d'interfaccia** scegliere la lingua che verrà utilizzata dall'amministratore creato.

- Nella lista a cascata **Formato della data** scegliere il formato, che verrà utilizzato da questo amministratore alla modifica delle impostazioni, che contengono date. Sono disponibili i seguenti formati:
  - europeo: `DD-MM-YYYY HH:MM:SS`
  - americano: `MM/DD/YYYY HH:MM:SS`
- Nel campo **Descrizione** si può impostare la descrizione personalizzata di utenza.
- In utenza amministratore di gruppi mettere il flag **Può amministrare un numero di gruppi limitato** per impostare i gruppi consentiti.

In questo caso diventa disponibile la sezione **Gruppi gestiti**. In questa sezione scegliere i gruppi di utenti, che verranno gestiti da questo amministratore. Per farlo, premere su nome gruppo nella lista **Gruppi conosciuti**. Per escludere dalla lista gruppi, gestiti da tale amministratore, premere su nome gruppo nella lista **Gruppi gestiti**.



I valori di campi, marcati con *, sono obbligatori da specificare.

4. Impostati tutti i parametri necessari, premere il tasto **Salva** per creare utenza amministratore.

## Eliminazione amministratore

***Per eliminare utenza amministratore:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Amministratori**.
2. Nella lista di amministratori scegliere un'utenza da eliminare.
3. Premere nella barra degli strumenti l'icona **Rimuovi l'account**.

## 5.3.2. Modifica amministratori

***Per modificare utenza amministratore:***

1. Aprire sezione impostazioni utenza.

   Per amministratori con i diritti completi si può fare in uno dei seguenti modi:

   - Scegliere la voce **Amministrazione** nel menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Amministratori**. Nella lista amministratori scegliere un'utenza da moficiare. Nella barra degli strumenti premere il tasto **Modifica**.
   - Scegliere la voce **Impostazioni** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce **Il mio account**.

   Per amministratori gruppi ed amministratori con i diritti di sola lettura le impostazioni utenza si aprono solo via la sezione **Impostazione** del menu principale del **Centro gestione**.

2. Se necessario, si possono modificare i parametri, impostati alla creazione di una nuova utenza.

   I valori di campi, marcati con *, sono obbligatori da specificare.

   Per amministratori gruppi e amministratori con i diritti di sola lettura la lista delle impostazioni modificabili è limitata.

3. I seguenti parametri sono di sola lettura:
   - Date creazione utenza e ultima modifica parametri,
   - **Stato** - visualizzo indirizzo di rete di ultima connessione sotto questa utenza.
4. Modificati i parametri, premere il tasto **Salva**.
5. Per modificare la password di utenza, scegliere nella barra degli strumenti l'icona **Nuova password**.



Amministratore con i diritti completi può modificare password di tutti gli altri amministratori.



Nella password amministratore non si possono utilizzare i caratteri nazionali.

# Capitolo 6. Gruppi. Gestione complessa di workstation

Gruppi sono destinati a semplificare la gestione di workstation di rete antivirus.

***Unificazione di workstation nei gruppi può essere utilizzata per:***

- Applicare le operazioni batch a tutte le workstation, che fanno parte di tale gruppo.

  Sia per un gruppo singolo, sia per alcuni gruppi scelti si possono avviare, visualizzare e sospendere i processi di scansione di workstation, che fanno parte di tale gruppo. Si possono inoltre visualizzare le statistiche (incl. infezioni, virus, avvio/fine, errori scansione e installazione ecc) e le statistiche totali per tutte le workstation di un gruppo o di più gruppi.

- Indicare le impostazioni uniche per le workstation via il gruppo, di cui fanno parte (v. voce Utilizzo dei gruppi per impostare le workstation).
- Organizzazione (strutturazione) della lista di workstation.

Si possono anche creare i gruppi innestati.

## 6.1. Gruppi di sistema e custom

### Gruppi di sistema

Durante l'installazione del **Server** vengono creati cosidetti gruppi (di sistema) predefiniti.

Inizialmente **Dr.Web Enterprise Security Suite** contiene un set di gruppi di sistema. Questi gruppi vengono creati durante l'installazione di **Enterprise Server** e non possono essere eliminati.

L'amministratore può comunque nasconderli, se necessario.

Ogni gruppo di sistema (oltre il gruppo **Everyone**) contiene un set di sottogruppi, raggruppati secondo un certo criterio.

## *Everyone*

Gruppo, che contiene tutte le workstation, note a **Enterprise Server**. Gruppo **Everyone** contiene le impostazioni predefinite.

## *Operating system*

Questa categoria di sottogruppi visualizza i sistemi operativi, sotto la gestione dei quali le workstation operano al momento. Questi gruppi non sono virtuali e non possono contenere le impostazioni di workstation, nonché essere i gruppi primari.

- Sottogruppi della famiglia **Android**. Questa famiglia include un set di gruppi, che corrispondono a una versione concreta del sistema operativo mobile Android.
- Sottogruppi della famiglia **MacOS X**. Questa famiglia include un set di gruppi, che corrispondono a una versione concreta del sistema operativo MacOS X.
- Sottogruppo **Netware**. Questo sottogruppo contiene le workstation, che operano sotto il sistema operativo Novell NetWare.
- Sottogruppi della famiglia **UNIX**. Questa famiglia include un set di gruppi, che corrispondono ai sistemi operativi della famiglia UNIX, per esempio, Linux, FreeBSD, Solaris ecc.
- Sottogruppi della famiglia **Windows**. Questa famiglia include un set di gruppi, che corrispondono alla versione concreta del sistema operativo Windows.
- Sottogruppo **Windows CE**. Questo sottogruppo contiene le workstation, che operano sotto il sistema operativo Windows Mobile.

## Status

Gruppo **Status** contiene gruppi innestati, che rispecchiano lo stato corrente di workstation: se sono connessi al momento al **Server** o meno, nonché lo stato del software antivirus: se il software antivirus è eliminato e se il periodo di validità è scaduto. Questi gruppi sono completamente virtuali e non possono contenere nessuna impostazione, nonché essere i gruppi primari.

- Gruppo **Deinstalled**. Non appena dalla workstation è eliminato il software **Enterprise Agent**, workstation passa al gruppo **Deinstalled**.
- Gruppo **Deleted**. Contiene le workstation, eliminate precedentemente dall'amministratore dal **Server**. Le workstation si possono ripristinare (v. voce Eliminazione e ripristino workstation).
- Gruppo **Offline**. Contiene tutte le workstation non connesse al momento.
- Gruppo **Online**. Contiene tutte le workstation connesse al momento (che reagiscono alle richieste del **Server**).

## Transport

Questi sottogruppi definiscono il protocollo, con cui le workstation sono connesse al momento al **Server**. I sottogruppi sono completamente virtuali e non possono contenere nessuna impostazione, e inoltre non possono essere i gruppi primari.

- Gruppo **TCP/IP**. Gruppo contiene le workstation, connesse al momento con il protocollo TCP/IP.
- Gruppo **TCP/IP Version 6**. Gruppo contiene le workstation, connesse al momento con il protocollo TCP/IP.
- Gruppo **IPX**. Gruppo contiene le workstation, connesse al momento con il protocollo IPX.
- Gruppo **NetBIOS**. Gruppo contiene le workstation, connesse al momento con il protocollo NetBIOS.

### *Ungrouped*

Questo gruppo contiene le workstation che non fanno parte dei gruppi custom.

## Gruppi custom

Sono i gruppi, definiti dall'amministratore della rete antivirus per le sue necessità. Amministratore può creare i propri gruppi, nonché i gruppi innestati, e aggiungerci le workstation. Da parte di **Dr.Web Enterprise Security Suite** non c'è nessuna limitazione di composizione né di nome di tali gruppi.

Per comodità nella tabella sotto sono riportati tutti gli eventuali gruppi e i tipi dei gruppi, nonché i parametri caratteristici, che sono supportati (+) o non sono supportati (–) da questi gruppi.

Sono presenti i seguenti parametri:

- **Appartenenza automatica**. Parametro definisce se le workstation possono essere aggiunte al gruppo automaticamente (supporto dell'appartenenza automatica) e se la composizione del gruppo può essere cambiata automaticamente durante l'operazione del **Server**.
- **Gestione appartenenza**. Parametro definisce se l'amministratore può gestire l'appartenenza al gruppo: aggiungendo o eliminando le workstation dal gruppo.
- **Gruppo primario**. Parametro definisce se questo gruppo è primario per la workstation.
- **Impostazioni**. Parametro definisce, se il gruppo può contenere le impostazioni di componenti antivirus (per passarle a workstation).

**Tabella 6-1. Gruppi e parametri supportati**

| Gruppo/tipo gruppi | Parametro | | | |
|---|---|---|---|---|
| | Appartenenza automatica | Gestione appartenenza | Gruppo primario | Impostazioni |
| Everyone | + | – | + | + |
| Status | + | – | – | – |
| Transport | + | – | – | – |
| Operating System | + | – | + | + |
| Ungrouped | + | – | – | – |
| Gruppi custom | – | + | + | + |



Sotto l'utenza dell'*Amministratore del gruppo* il gruppo custom, da esso gestito, viene visualizzato nella radice di albero gerarchico, anche se effettivamente ha un gruppo padre. In questo caso sono disponibili tutti i gruppi figli del gruppo gestito.

# 6.2. Gestione gruppi

## 6.2.1. Creazione e eliminazione gruppi

### Creazione del gruppo

***Per creare un nuovo gruppo:***

1. Scegliere la voce  **Si può aggiungere una postazione o un gruppo** nella barra degli strumenti, dopo nel sottomenu scegliere la voce  Creare gruppo.

   Si apre la finestra di creazione del gruppo.

2. Campo di input **Identificatore** viene compilato automaticamente. Se necessario, si può modificarlo durante la creazione. Identificatore non deve contenere spazi. Di seguito identificatore del gruppo non può essere modificato.
3. Indicare nel campo **Nome** il nome del gruppo.
4. Per i sottogruppi nel campo **Gruppo padre** scegliere nella lista a cascata il gruppo da considerare il gruppo padre, dal quale viene ereditata la configurazione, se non sono indicate le impostazioni personalizzate. Per il gruppo radice (che non ha padre) lasciare questo campo vuoto, il gruppo viene aggiunto alla radice della lista gerarchica. In questo caso le impostazioni vengono ereditate dal gruppo **Everyone**.
5. Inserire un commento nel campo **Descrizione**.Premere il tasto **Salva**.

I gruppi creati sono inizialmente vuoti. Come si aggiungono le workstation in gruppi è descritto nella sezione Aggiungimento di workstation al gruppo. Eliminazione di workstation dal gruppo.

## Eliminazione del gruppo

***Per eliminare il gruppo esistente:***

1. Scegliere il gruppo custom nella lista gerarchica di **Centro gestione**.
2. Nella barra degli strumenti premere **Generali** → **Rimuovere gli oggetti segnalati**.

> I gruppi predefiniti non si possono eliminare.

## 6.2.2. Impostazioni di gruppi

***Per configurare i gruppi:***

1. Scegliere la voce **Rete antivirus** del menu principale di **Centro gestione**, nella finestra aperta nella lista gerarchica scegliere il gruppo.
2. Premere la voce **Proprietà** nel menu di gestione (pannello a sinistra).
3. Si apre la finestra con le proprietà del gruppo. Questa finestra contiene le schede **Generali** e **Configurazione**. I loro contenuti e la loro configurazione sono descritti sotto.



Se si aprono le proprietà del gruppo via la voce  **Generali** →  **Modificare** nella barra degli strumenti, è inoltre disponibile la sezione **Informazioni sulle postazioni**, in cui si trova l'informazione generale sulle workstation, che fanno parte di tale gruppo.

4. Per salvare le modifiche apportate, premere il tasto **Salva**.

## Generali

Nella sezione **Generali** ci sono i campi seguenti:

- **Identificatore** - identificatore unico del gruppo. Non modificabile.
- **Nome** - nome del gruppo. Se necessario, si può modificare il nome del gruppo.



Nei gruppi predefiniti i campi **Identificatore** e **Nome** non sono modificabili.

- **Gruppo padre** - gruppo padre, di cui fa parte tale gruppo e dal quale eredita la sua configurazione, se non ce ne sono delle impostazioni personalizzate. Se il gruppo padre non è impostato, le impostazioni vengono ereditate dal gruppo **Everyone**.

- **Descrizione** - campo non obbligatorio con la descrizione del gruppo.

## Configurazione



Per le informazioni dettagliate su ereditarietà di impostazioni dei gruppi da workstation, per cui tale gruppo è primario, v. sezione Utilizzo di gruppi per configurazione di workstation.

Nella sezione **Configurazione** ci sono impostazioni del gruppo, che includono:

-  - impostazione di diritti di utenti di workstation, per cui tale gruppo è primario. Impostazione di diritti è simile all'impostazione di diritti di workstation singole (v. voce Impostazione diritti utenti).
-  - impostazione di orario di avvio di processi di workstation, per cui tale gruppo è primario. Impostazione di orario del gruppo è simile all'impostazione di orario centralizzato delle workstation (v. voce Impostazione orari di processi su workstation).
-  - impostazione di chiave di licenza di workstation, per cui tale gruppo è primario.
-  - impostazione di limitazioni dell'aggiornamento del software antivirus di workstation, per cui tale gruppo è primario (v. voce Limitazione aggiornamenti).
-  - lista dei componenti, installati sulle workstation, per cui tale gruppo è primario. Modifica della lista di componenti dei gruppi è simile alla modifica della lista di componenti di workstation (v. voce Contenuti pacchetto antivirus).
- Impostazioni dei componenti del pacchetto antivirus: **Dr.Web Scanner per Windows**, **SpIDer Guard G3 per Windows**, **SpIDer Mail per postazioni Windows** ecc. Per modificare le impostazioni, premere il tasto  vicino al componente corrispondente. Configurazione di componenti del pacchetto antivirus del gruppo è simile alla configurazione dei componenti di workstation (v. anche la voce Configurazione workstation).

# 6.3. Aggiungere workstation al gruppo. Eliminare workstation dal gruppo

Ci sono alcuni modi di aggiungere le workstation ai gruppi custom:

1. Modificare le impostazioni di workstation.
2. Trascinare la workstation nella lista gerarchica (drag'n'drop).

***Per modificare la lista dei gruppi, di cui fa parte la workstation, via le impostazioni di workstation:***

1. Scegliere la voce **Rete antivirus** del menu principale, nella finestra aperta nella lista gerarchica cliccare sul nome di workstation.
2. Aprire la sezione di impostazioni di workstation in uno dei seguenti modi:
   - Nel menu di gestione (pannello a sinistra) scegliere la voce **Proprietà**.
   - Premere **Generali** → **Modificare** nella barra degli strumenti.
3. Nel pannello aperto **Proprietà** passare alla sezione (alla scheda) **Gruppi**.

   Nella lista **Appartenenza a** sono elencati i gruppi, di cui workstation già fa parte.

   Nella lista **Lista di gruppi** si trova la lista di tutti gli altri gruppi custom.

4. Per aggiungere la workstation al gruppo custom, cliccare sul suo nome nella lista **Lista di gruppi**. La workstation viene aggiunta a questo gruppo, e il gruppo viene spostato nella lista **Appartenenza a**.
5. Per eliminare la workstation dal gruppo custom, cliccare sul nome gruppo nella lista **Appartenenza a**. La workstation viene eliminata dal gruppo, e il gruppo viene spostato nella lista **Lista di gruppi**.



Eliminazione di workstation dai gruppi predefiniti non è possibile.

6. Per salvare le modifiche apportate, premere il tasto **Salva**.

Inoltre nella sezione proprietà workstation si può impostare il gruppo primario per la workstation (per più informazioni v. Ereditarietà di elementi di configurazione di workstation. Gruppi primari).

***Per modificare la lista dei gruppi, di cui fa parte la workstation, via la lista gerarchica:***

1. Scegliere la voce **Rete antivirus** del menu principale e aprire la lista gerarchica di gruppi e workstation.
2. Per aggiungere la workstation al gruppo custom, premere il tasto CTRL e trascinare la workstation con il mouse nel gruppo necessario (drag'n'drop).
3. Per spostare la workstation da un gruppo custom all'altro, trascinare la workstation con il mouse (drag'n'drop) dal gruppo custom, da cui la workstation viene eliminata, al gruppo custom, dove la workstation viene aggiunta.



Al trascinamento di workstation dal gruppo predefinito secondo la voce 2 o 3, la workstation viene aggiunta al gruppo custom e non viene eliminata dal gruppo predefinito.



Tale metodo (drag'n'drop) non funziona se si utilizza il browser web Windows Internet Explorer 7.

## *Unificazione di workstation*

Dopo le operazioni con il database o alla reinstallazione del software delle workstation antivirus, nella lista gerarchica della rete antivirus possono essere più workstation con lo stesso nome (solo uno di questi sarà correlato con la workstation antivirus corrispondente).

***Per eliminare i nomi doppi di workstation:***

1. Scegliere i nomi doppi di una workstation. Per farlo, utilizzare il tasto CTRL.
2. Nella barra degli strumenti scegliere **Generali** → **Unire le postazioni**.
3. Nella lista proposta scegliere la workstation da considerare workstation master. Tutte altre workstation saranno eliminate, e i loro dati saranno attribuiti a quella scelta.
4. Nella lista proposta scegliere la workstation, le cui impostazioni saranno definite per la workstation master scelta.
5. Premere **Salva**.

# 6.4. Utilizzo dei gruppi per impostare le workstation

***Impostazioni di workstation possono essere:***

1. Ereditate dal gruppo primario.
2. Impostate personalmente.

## Ereditarietà delle impostazioni

Alla creazione di un nuovo gruppo le sue impostazioni vengono ereditate dal gruppo padre o dal gruppo **Everyone**, se il gruppo padre non è impostato.

Alla creazione di una nuova workstation le sue impostazioni vengono ereditate dal gruppo primario.



Per più informazioni v. voce Ereditarietà di elementi di configurazione di workstation. Gruppi primari.

Alla visualizzazione o alla modifica di elementi di configurazione di workstation, ereditati dal gruppo primario, nelle finestre corispondenti

viene visualizzata l'informazione che tale impostazione è ereditata dal gruppo primario.

Si possono impostare varie configurazioni per i vari gruppi e workstation, modificando le impostazioni corrispondenti.

## Impostazioni individuali

Per indicare le impostazioni personalizzate di workstation, modificare la sezione corrispondente di impostazioni (v. voce Configurazione workstation). In questo caso nella sezione impostazioni viene visualizzata l'informazione che tale impostazione è personalizzata per questa workstation.

Se la workstation ha delle impostazioni personalizzate, le impostazioni del gruppo primario ed eventuali modifiche di esse non influiranno sulle impostazioni di workstation.

Si può ripristinare la configurazione, ereditata dal gruppo primario. Per farlo, premere il tasto **Rimuovi queste impostazioni** nella barra degli strumenti di **Centro gestione** nella sezione di impostazioni corrispondenti o nella sezione proprietà di workstation.

# 6.4.1. Ereditarietà di elementi di configurazione di workstation. Gruppi primari

## Ereditarietà di impostazioni

Alla creazione di una workstation nuova i suoi elementi di configurazione vengono ereditati da uno dei gruppi, di cui fa parte. Tale gruppo si chiama *primario*.Se vengono modificate le impostazioni del gruppo primario, le modifiche vengono ereditate da workstation che fanno parte del gruppo, salvo che le workstation avevano le impostazioni personalizzate. Alla creazione di workstation si può indicare, quale gruppo è da considerare primario. Di default è il gruppo **Everyone**.

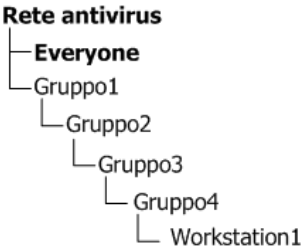
Se il gruppo primario non è **Everyone** e il gruppo primario indicato non ha le impostazioni personalizzate, vengono ereditate le impostazioni del gruppo **Everyone**.

Si possono creare i gruppi innestati.

Se ci sono i gruppi innestati e la workstation non ha le impostazioni personalizzate, l'ereditarietà di elementi di configurazione avviene secondo la struttura di gruppi innestati. La ricerca viene eseguita dal basso in alto di albero gerarchico, partendo dal gruppo primario, dal suo gruppo padre e fino all'elemento radice dell'albero. Se non sono state rilevate le impostazioni personalizzate, vengono ereditati gli elementi di configurazione del gruppo **Everyone**.

**Per esempio:**

La struttura della lista gerarchica rappresenta un seguente albero:




Gruppo `Group4` non è primario per la workstation `Station1`. All'ereditarietà delle impostazioni di workstation `Station1` parte la ricerca delle impostazioni nel seguente ordine: `Station1` → `Group4` → `Group3` → `Group2` → `Group1` → `Everyone`.

Di default la struttura di rete viene visualizzata, dimostrando l'appartenenza di workstation a tutti i gruppi, di cui essa fa parte. Se si vuole visualizzare nella cartella l'appartenenza di workstation solo ai gruppi primari, nella barra degli strumenti di **Centro gestione** nella voce **Impostazioni del tipo albero** togliere il flag

**Appartenenza a tutti i gruppi**.

## Impostazione del gruppo primario

Ci sono alcuni modi per impostare il gruppo primario per la workstation e per il gruppo di workstation.

### *Per impostare il gruppo primario per la workstation:*

1. Scegliere la voce **Rete antivirus** del menu principale, nella finestra aperta nella lista gerarchica premere sul nome workstation.
2. Nel menu di gestione (pannello a sinistra) scegliere la voce **Proprietà**. Nella finestra aperta passare alla scheda **Gruppi**.
3. Se è necessario impostare altro gruppo primario, premere l'icona del gruppo della lista **Appartenenza a**.
4. Premere il tasto **Salva**.

### *Per impostare il gruppo primario per più workstation:*

1. Scegliere la voce **Rete antivirus** del menu principale, nella finestra aperta nella lista gerarchica cliccare sui nomi di workstation richieste (si possono inoltre scegliere i gruppi per applicare l'azione a tutte le workstation che ne fanno parte), si possono scegliere più workstation e gruppi con il mouse, tenendo schiacciati i tasti CTRL o SHIFT.
2. Nella barra degli strumenti premere **Generali** → **Impostare queste gruppo come primario**. Si apre la finestra con la lista dei gruppi che si possono impostare come primari per queste workstation.
3. Per indicare il gruppo primario, cliccare sul nome del gruppo.

Si può impostare il gruppo come primario per tutte le workstation che ne fanno parte. Per farlo, scegliere il gruppo richiesto nella cartella, dopodiché nella barra degli strumenti di **Centro gestione** premere **Generali** → **Impostare il gruppo primario**.

### 6.4.2. Copiare le impostazioni in altri gruppi / workstation

Impostazioni di configurazione di mezzi antivirus, di orari, di diritti utenti e di altri impostazioni di gruppo o di workstation possono essere copiate in (applicate a) gruppo o in più gruppi e workstation.

***Per copiare le impostazioni:***

1. Premere il tasto **Propaga queste impostazioni verso un altro oggetto**:
   -  nella finestra di modifica di configurazione del componente antivirus,
   -  nella finestra di modifica dell'orario,
   -  nella finestra di configurazione di limitazioni di aggiornamento,
   -  nella finestra dei componenti installati.

   Si apre la finestra della cartella di rete.
2. Scegliere nella lista i gruppi e le workstation a cui si vuole applicare l'impostazione.
3. Per poter apportare le modifiche alla configurazione di questi gruppi, premere il pulsante **Salva.**

## 6.5. Comparazione workstation e gruppi

Si possono comparare le workstation e i gruppi per i parametri principali.

***Per comparare alcuni oggetti della rete antivirus:***

1. Scegliere la voce **Rete antivirus** nel menu principale, nella finestra aperta nella lista gerarchica scegliere gli oggetti da comparare. Utilizzare i tasti CTRL e SHIFT. Sono possibili le seguenti varianti:

- scelta di alcune workstation - per comparare le workstation scelte;
- scelta di alcuni gruppi - per comparare i gruppi scelti e tutti i sottogruppi;
- scelta di alcuni workstation e gruppi - per comparare tutte le workstation: sia scelte direttamente nella lista gerarchica, sia quelle che fanno parte dei gruppi scelti e di tutti i sottogruppi.

2. Nel menu di gestione (pannello a sinistra) premere la voce **Comparazione.**
3. Si apre la tabella comparativa con oggetti scelti.

- Parametri comparazione per i gruppi:
  - **Postazione** - numero totale di workstation che fanno parte del gruppo.
  - **Postazione nella rete** - numero workstation, attive al momento.
  - **Gruppo primario per** - numero workstation, per cui il gruppo scelto è primario.
  - **Impostazioni individuali** - lista dei componenti, che hanno le impostazioni personalizzate, non ereditate dal gruppo padre.
- Parametri comparazione per le workstation:
  - **Data di creazione** workstation.
  - **Gruppo primario** per la workstation.
  - **Impostazioni individuali** - lista dei componenti, per cui sono configurate le impostazioni personalizzate, non ereditate dal gruppo primario.
  - **Componenti installati** - lista dei componenti antivirus, installati sulla workstation.

# Capitolo 7. Gestione workstation

Rete antivirus che opera sotto la gestione di **Dr.Web Enterprise Security Suite** permette di configurare nel modo centralizzato pacchetti antivirus su workstation. **Dr.Web Enterprise Security Suite** permette di:

- configurare i parametri di strumenti antivirus,
- configurare l'orario di avvio di processi di scansione,
- avviare i processi singoli su workstation nonostante le impostazioni di orario,
- avviare il processo di aggiornamento di workstation, compreso dopo quello di errore di aggiornamento con resettaggio dello stato errore.

In questo caso l'amministratore della rete antivirus può lasciare all'utente di workstation le abilitazioni per la configurazione indipendente e per l'avvio di processi, proibire tali attività o limitarle notevolmente.

Le modifiche nella configurazione di workstation si possono apportare perfino quando la workstation è provvisoriamente non raggiungibile per il **Server**. Queste modifiche saranno accettate da workstation non appena la sua connessione al **Server** viene ripristinata.

# 7.1. Gestione record di workstation

## 7.1.1. Politica di connessione workstation



La procedura di creazione di workstation via **Centro gestione** è descritta nella voce Creazione utenza nuova.

La possibilità di gestire l'autorizzazione workstation su **Enterprise Server** dipende dai seguenti parametri:

1. Se durante l'installazione di **Agent** su workstation è stata scelta la variante di autorizzazione **Automaticamente**, la modalità di accesso di workstation al **Server** verrà definita secondo le impostazioni, indicate sul **Server** (predefinita), v. sotto.
2. Se durante l'installazione di **Agent** su workstation è stata scelta la variante di autorizzazione **Manuale** e sono impostati i parametri **Identificatore** e **Password**, alla connessione al **Server** workstation verrà autorizzata automaticamente indipendentemente dalle impostazioni del **Server** (predefinita se **Agent** viene installato via pacchetto di installazione *esinst* - v. File di installazione).



Impostazione del tipo di autorizzazione di **Agent** alla sua installazione è descritta nella sezione Installazione di Dr.Web Enterprise Agent nella modalità grafica di installazione (passo 6).

***Per modificare la modalità dell'accesso di workstation a Dr.Web Enterprise Server:***

1. Aprire le configurazioni del **Server**. Per farlo, scegliere la voce **Amministrazione** del menu principale, nella finestra aperta scegliere la voce del menu di gesione **Configurazione Dr.Web Enterprise Server**.
2. Nella scheda **Generali** nella lista a cascata **Nuovi arrivi**

scegliere uno dei seguenti valori:

- **Confermare l'accesso a mano** (modalità predefinita, se non modificata all'installazione del **Server**),
- **Consentire l'accesso automaticamente**,
- **Sempre negare l'accesso**.

## Conferma di accesso manuale

Nella modalità **Conferma di accesso manuale** le workstation nuove vengono messe nella lista di workstation non confermate per la revisione diretta dell'amministratore.

***Per accedere alla lista di workstation non confermate:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Postazioni non confermate**.
2. Nella finestra aperta viene visualizzata la tabella di workstation con **Agent** installati che richiedono l'accesso al **Server**, nonché l'informazione generale su workstation: tempo di ricezione della richiesta, nome di rete di workstation, indirizzo IP di workstation e SO installato su workstation.
3. Per impostare l'accesso al **Server** mettere i flag sulle workstation richieste o mettere il flag nell'intestazione della tabella per marcare tutte le workstation. Nella barra degli strumenti scegliere l'azione da applicare a workstation scelte:
   -  - consentire l'accesso a workstation scelte e impostare il gruppo primario dalla lista proposta,
   -  - negare l'accesso a workstation scelte.

## Consentire automaticamente l'accesso

Nella modalità **Consentire l'accesso automaticamente** tutte le workstation che richiedono l'accesso al **Server** vengono connesse automaticamente senza ulteriori richieste all'amministratore. In questo caso come gruppo primario viene impostato il gruppo **Everyone**.

## Negazione accesso

Nella modalità **Sempre negare l'accesso** il **Server** nega l'accesso se riceve le richieste di workstation nuove. L'amministratore deve creare i record di workstation manualmente e assegnarle le password di accesso.

## 7.1.2. Eliminazione e ripristino workstation

***Per eliminare record di una workstation:***

1. Per eliminare una workstation via il **Centro gestione**: scegliere la voce del menu principale **Rete antivirus**, nella finestra aperta premere nella barra degli strumenti **Generali** → **Rimuovere gli oggetti segnalatti**.
2. Si apre la finestra di conferma di eliminazione di workstation. Premere su **OK**.

Dopo l'eliminazione di workstation dalla lista gerarchica esse vengono messe nella tabella di workstation eliminate, da dove si possono ripristinare gli oggetti via il **Centro gestione**.

***Per ripristinare un record di workstation:***

1. Scegliere la voce del menu principale **Rete antivirus**, nella finestra aperta nella lista gerarchica scegliere una o più workstation eliminate da ripristinare.

> Tutte le workstation eliminate si trovano nel sottogruppo **Deleted** del gruppo **Status**.

2. Nella barra degli strumenti scegliere la voce **Generali** → **Ripristinare le postazioni rimosse**.
3. Si apre la sezione del ripristino di workstation eliminate. Si possono configurare i seguenti parametri di workstation, che verranno impostati al ripristino:

- **Gruppo primario** - scegliere il gruppo primario a cui aggiungere la workstation ripristinata. Di default è scelto il gruppo primario impostato per la workstation alla sua eliminazione.



Al ripristino contemporaneo di più workstation di default è scelta la variante **L'ex gruppo primario** che significa che per ogni workstation scelta viene impostato il suo gruppo primario, a cui la workstation apparteneva prima dell'eliminazione. Se si sceglie un gruppo concreto, per tutte le workstation ripristinate viene impostato lo stesso gruppo scelto.

- Nella sezione **Appartenenza a** si può modificare la lista dei gruppi, a cui appartiene la workstation. Di default è impostata la lista dei gruppi, a cui la workstation apparteneva prima dell'eliminazione. Per aggiungere la workstation ai gruppi custom, premere su nome dei gruppi custom disponibili nella sezione **Lista gruppi**. Per escludere i gruppi custom, a cui la workstation apparteneva prima dell'eliminazione, premere su nomi dei gruppi corrispondenti nella sezione **Appartenenza a**.

4. Per ripristinare workstation con parametri impostati premere il tasto **Recuperare**.

# 7.2. Configurazione workstation

## Proprietà workstation

***Per visualizzare e modificare le proprietà di workstation:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica scegliere la workstation e premere su **Generali** → **Modificare** nella barra degli strumenti.
2. Nella parte destra della finestra del **Centro gestione** si apre la finestra con le proprietà di workstation. Questa finestra contiene i seguenti gruppi di impostazioni: **Generali**,

**Configurazione**, **Gruppi**, **Sicurezza**, **Posizione**. I loro contenuti e la loro configurazione sono descritti sotto.

3. Per salvare le modifiche apportate premere sul tasto **Salva**.

## *Generali*

Nella sezione **Generali** sono riportati i seguenti campi, disponibili solo per la lettura:

- **Identificatore** – identificatore unico di workstation.
- **Nome** – nome workstation.

Si possono impostare i valori dei seguenti campi::

- Nel campo **Password** impostare la password per autorizzazione di workstation sul **Server** (si deve ripetere la stessa password nel campo **Password ripetuta**). Al cambio della password, per poter connettere **Agent**, la stessa procedura deve essere eseguita nelle impostazioni di connessione di **Agent** su workstation.
- Nel campo **Descrizione** aggiungere le informazioni supplementari.



I valori dei campi, marcati con il carattere *, devono essere obbligatoriamente impostati.

## *Configurazione*

Nella sezione **Configurazione** si può modificare la configurazione di questa workstation, che comprende:

-  - configurazione dei diritti di utente di workstation (v. Configurazione diritti utenti).
-  - configurazione di orario di avvio di processi su workstation. Descrizione di impostazione di orario centralizzato è riportata in Configurazione orario processi su workstation.
-  - impostazione della chiave di licenza su workstation.

-  - configurazione limitazioni all'aggiornamento del software antivirus. Descrizione di configurazione di aggiornamenti è riportata in Limitazione aggiornamenti workstation.
-  - lista dei componenti installati (v. Contenuti pacchetto antivirus).
- Configurazione dei componenti del pacchetto antivirus - **Dr.Web Scanner per Windows**, **SpIDer Guard G3 per Windows**, **SpIDer Mail per le workstation Windows** ecc. Per applicare le configurazioni premere sul tasto  accanto al componente corrispondente.

Dal **Centro gestione** sono inoltre disponibili i tasti per eliminare le impostazioni personali. Sono locati a destra dei tasti di configurazione corrispondenti. All'eliminazione della configurazione personalizzata viene di nuovo ripristinata la configurazione, ereditata dal gruppo primario.



Composizione dei parametri di componenti e i consigli su loro configurazione sono contenuti nel manuale **Dr.Web® Anti-virus per Windows. Manuale dell'utente**, ed anche **Dr.Web® Agent per Windows. Manuale dell'utente**.

Nello stesso tempo, la gestione delle configurazioni via il **Centro gestione** è diversa dalla gestione di impostazioni diretta via i componenti corrispondenti di antivirus:

- per modificare i valori dei parametri, che hanno valori **Sì** o **No**, cliccare sul valore corrispondente. I campi di input e le liste a cascata hanno l'interfaccia standard,
- per gestire i singoli parametri utilizzare i tasti, locati a destra delle impostazioni corrispondenti:

   - ripristinare il valore del parametro precedente alla modifica,

   - ripristinare il valore predefinito del parametro,
- per gestire il complesso dei parametri utilizzare i tasti nella barra degli strumenti (parte superiore della maggior parte delle finestre di impostazioni, per esempio, **Permessi, Orario**,

**Dr.Web Scanner per Windows**, **SpIDer Guard per Windows** e **SpIDer Mail per postazioni Windows**):

 - estendere queste configurazioni su altri oggetti (gruppo o più gruppi e workstation),

 - ripristinare i valori di tutti i parametri precedenti alla modifica,

 - ripristinare per tutti i parametri i valori predefiniti,

 - esportare i parametri nel file del formato speciale,

 - importare i parametri dal file del formato speciale,

 - eliminare la configurazione personalizzata per tale workstation (in questo caso viene di nuovo ripristinata la configurazione, ereditata da gruppi, v. Utilizzo gruppi per configurazione workstation).

- Premere sul tasto **Salva** per accettare le modifiche apportate.

## *Gruppi*

Nella sezione **Gruppi** viene impostata la lista dei gruppi, di cui fa parte tale workstation (v. Aggiungere workstation al Gruppo. Eliminazione di workstation dal gruppo).

Inoltre in questa sezione si può modificare il gruppo primario per workstation (v. Ereditarietà elementi configurazione workstation. Gruppi primari).

## *Sicurezza*

Nella sezione **Sicurezza** vengono impostate le limitazioni di indirizzi di rete, da cui è consentito l'accesso a tale workstation.

Per consentire tutte le connessioni, togliere il flag **Usa questa lista del'accesso**. Per applicare le liste di indirizzi consentiti o bloccati, mettere questo flag.

Per consentire accesso da un certo indirizzo TCP, includerlo nella lista

**TCP: permesso** o **TCPv6: permesso**.

Per bloccare qualche indirizzo TCP, includerlo nella lista **TCP: prohibito** o **TCPv6: prohibito**.

### *Per modificare indirizzi nella lista:*

1. Inserire indirizzo di rete nel campo corrispondente e premere sul tasto **Salva**.
2. Per aggiungere nuovo campo di indirizzo, premere sul tasto  della sezione corrispondente.
3. Per eliminare il campo premere sul tasto  .

   Indirizzo di rete viene impostato nel formato: *<indirizzo-IP>*/[*<prefisso>*].

**Esempio di utilizzo del prefisso:**

1. Prefisso 24 definisce le reti con la maschera: `255.255.255.0`

   Contiene 254 indirizzi

   Indirizzi di host in queste reti del tipo: `195.136.12.*`

2. Prefisso 8 definisce le reti con la maschera `255.0.0.0`

   Contiene fino a 16387064 indirizzi (256*256*256)

   Indirizzi di host in queste reti del tipo: `125.*.*.*`

Inoltre si possono eliminare gli indirizzi dalla lista e modificare gli indirizzi inseriti nella lista.

Nello stesso modo vengono configurate le restrizioni di indirizzi IPX.

Indirizzi, non compresi in nessuna lista, sono consentiti o bloccati a seconda del flag posto o no **Priorità del divieto**: con il flag posto gli indirizzi, non compresi in nessuna lista (o compresi in tutti e due), sono bloccati. Nel caso contrario tali indirizzi vengono consentiti.

### *Posizione*

Nella sezione **Posizione** si impostano i parametri di posizione geografica di workstation.



Si possono creare vari gruppi di utenti a secondo quali diritti e impostazioni sono ottimali per essi. Impostazione dei parametri principali di operazione di workstation via gruppi permette di risparmiare le forze sulla modifica delle configurazioni di ogni singola workstation.

## Eliminazione di configurazioni di workstation

***Per eliminare le configurazioni personali di workstation:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica scegliere la workstation e premere nella barra degli strumenti  **Generali** →  **Rimuovere le impostazioni individuali dell'oggetto**. Si apre la finestra delle configurazioni di questa workstation, le configurazioni personalizzate saranno marcati con i flag.
2. Dalle configurazioni da eliminare togliere i flag richiesti e premere su **Salva**. Le configurazioni di workstation, ereditate dal gruppo primario, verranno ripristinati.



Alla modifica di configurazione di workstation per i componenti di **SpIDer Guard per Windows**, e anche **Dr.Web Scanner per Windows** leggere le istruzioni di utilizzo dei programmi antivirus per i computer sotto la gestione del SO Windows Server 2003, del SO Windows 2000 e del SO Windows XP. L'articolo che contiene le informazioni necessarie si trova all'indirizzo - http://support.microsoft.com/kb/822158/it. Materiale di questo articolo è volto ad ottimizzare il rendimento del sistema.

A condizione che la chiave di **Agent** (`agent.key`) consenta l'utilizzo del filtro spam per il componente **SpIDer Mail**, nella scheda **Antispam** si può eseguire l'impostazione del filtro (scegliere nel menu contestuale di qualsiasi gruppo o workstation la voce **SpIDer Mail per postazioni Windows**).

Partendo dalla versione **5.0** nei contenuti del pacchetto antivirus di **Dr.Web Enterprise Security Suite** rientrano i prodotti **SpIDer Gate** e **Controllo Ufficio**, per poter utilizzare i quali è inoltre necessario che essi siano indicati nella licenza (**Antivirus + Antispam**), che si può visualizzare nella chiave di **Agent**.

Descrizione delle configurazioni del filtro spam, nonché dei componenti **SpIDer Gate** e **Controllo Ufficio** viene riportata nel manuale **Dr.Web® Anti-virus per Windows. Manuale dell'utente**.

## 7.2.1. Configurazione diritti utenti

***Per impostare i diritti di utenti di workstation con il Centro gestione di Dr.Web:***

1. Scegliere la voce **Rete antivirus** del menu principale, nella finestra aperta nella lista gerarchica premere sul nome di workstation. Nel menu aperto di gestione (pannello a sinistra) scegliere la voce **Permessii**. Si apre la finestra di impostazione di diritti.
2. Modifica delle regole è eseguita nelle seguenti schede:
   - **Componenti** - impostazione di diritti per gestire i componenti antivirus. Di default all'utente rimangono i diritti di avvio di ogni componente, ma gli è vietato modificare la configurazione dei componenti ed arrestarli.
   - **Generali** - configurazione dei diritti della gestione di **Enterprise Agent** e delle sue funzionalità:
     - **Modalità mobile e utilizzo del Sistema globale d'aggiornamento Dr.Web** - disattiva la voce **Modalità mobile** nel menu contestuale di **Agent**.

- **Creazione dell'orario locale** - disattiva la voce **Locale** nel gruppo di impostazioni **Orario** nel menu contestuale di **Agent**.
- **Cambio delle modalità di operazione** - disattiva la voce **Modalità** e gruppo impostazioni **Componenti installati** nel menu contestuale di **Agent**.
- **Cambio delle impostazioni di Dr.Web Enterprise Agent** - disattiva nel menu contestuale di **Agent**, nel gruppo di impostazioni **Impostazioni** la voce **Sincronizzare ora** e gruppo impostazioni del **Livello log.**
- **Interruzione dell'interfaccia di Dr.Web Enterprise Agent** - disattiva la voce **Uscire** nel menu contestuale dell'**Agent**, se l'interfaccia di **Agent** è avviata sotto l'utente senza i diritti dell'amministratore.
- **Vietare l'accesso alla rete** - disattiva la voce **Accesso alla rete** nel menu contestuale dell'**Agent**.
- **Disabilitare la protezione del sistema** - disattiva il gruppo delle impostazioni **Protezione sistema** nel menu contestuale dell'**Agent**.
- **Sospensione di auto-difesa** - disattiva attività della voce **Autoprotezione** del menu contestuale di **Agent**.
- **Disinstallazione di Dr.Web Agent** - vieta eliminazione di **Agent** da workstation sia con installazione, sia con strumenti standard del SO Windows (v. Eliminazione dei componenti del software per i SO Windows®). In questo caso l'eliminazione di **Agent** può essere eseguito solo con la voce  **Generali** →  **Disinstalla Dr.Web Enterprise Agent** nella barra degli strumenti del **Centro gestione**.

Per modificare (attivare o disattivare) qualsiasi diritto, mettere o togliere il seguente flag.



Alla disattivazione di qualsiasi voce della modifica di configurazioni di **Agent** viene utilizzato il valore impostato per tale configurazione la volta precedente alla disattivazione.

Descrizione di azioni, eseguite dalle voci corrispondenti del menu, è riportata nella documentazione di **Dr.Web® Agent per Windows. Manuale dell'utente**.

3. Per annullare tale configurazione di diritti e tornare alla configurazione predefinita, ereditata dai gruppi predefiniti, premere sul tasto **Rimuovi queste impostazioni**.
4. Queste impostazioni si possono estendere su altro oggetto, premendo sul tasto .
5. Per esportare queste impostazioni nel file, premere su .
6. Per importare tali impostazioni dal file, premere su .
7. Per accettare le modifiche di diritti fatti premere sul tasto **Salva**.

Se al momento di modifica delle impostazioni di workstation essa non è connessa al **Server**, le modifiche saranno accettate quando l'**Agent** ripristina la connessione al **Server**.

## 7.2.2. Visualizzazione componenti installati del pacchetto antivirus

### Componenti

***Per sapere, quali componenti del pacchetto antivirus sono installati su workstation:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo.
2. Nel menu di gestione aperto (pannello a sinistra) scegliere la voce **Componenti installati**. Si apre la finestra con la lista dei componenti installati.



Lista dei componenti installati dipende da:

- Componenti, il cui utilizzo è consentito nel file della chiave.
- SO di workstation.
- Configurazioni, impostate dall'Amministratore sul **Server** della rete antivirus. L'Amministratore può modificare la composizione dei componenti del pacchetto antivirus su workstation sia prima dell'installazione di **Agent**, sia in qualsiasi momento dopo la sua installazione (v. Contenuti pacchetto antivirus).



Sui server, che eseguono le funzioni importanti di rete (controller di dominio, server di distribuzione licenze ecc), non si consiglia di installare i componenti **SpIDer Gate**, **SpIDer Mail** e **Dr.Web Firewall** per evitare eventuali conflitti dei servizi di rete e di componenti interni di **Dr.Web** Anti-virus.

## Database dei virus

***Per sapere, quali database dei virus sono installati su workstation:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation. Nel menu di gestione aperto (pannello a sinistra) scegliere dalla sottosezione **Tabella** la voce **Basi virali**.
2. Si apre la finestra di informazione con le informazioni sui database dei virus installati: nome file, che contiene un database dei virus concreto; versione database dei virus; numero scritture nel database dei virus; data creazione database.



Se la visualizzazione della voce **Database dei virus** è disattivata, per attivarlo scegliere la voce **Amministrazione** del menu principale, nella finestra aperta scegliere la voce del menu di gestione **Configurazione di Dr.Web Enterprise Server**. Nella scheda **Informazione statistiche** mettere il flag **Monitoraggio delle basi di dati di virus** e **Monitoraggio dello stato delle postazioni**, dopodiché riavviare il **Server**.

## 7.2.3. Contenuti pacchetto antivirus

***Per configurare la lista di componenti installati del pacchetto antivirus:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica scegliere workstation o gruppo. Nel menu di gestione aperto (pannello a sinistra) scegliere la voce **Componenti da installare**.
2. Per i componenti richiesti scegliere nella lista a cascata una delle varianti:
   - **deve** - imposta la presenza obbligatoria del componente su workstation. Alla creazione di una nuova workstation il componente fa parte del paccheto antivirus installato nel modo obbligatorio. All'impostazione del valore **deve** di una workstation già esistente il componente viene aggiunto ai contenuti del pacchetto antivirus attuale;
   - **può** - imposta la possibilità di installazione del pacchetto antivirus. La decisione di installazione viene presa dall'utente;
   - **non può** - blocca la presenza del componente su workstation. Alla creazione di una nuova workstation il componente non fa parte dei contenuti del pacchetto antivirus installato. All'impostazione del valore **non può**per una workstation già esistente il componente viene eliminato dai contenuti del pacchetto antivirus.

   Nella tabella 7-1 è indicato se viene installato il componente su

workstation (+) a seconda dei parametri, impostati dall'utente, e delle configurazioni, impostati dall'amministratore sul **Server**.

**Tabella 7-1.**

| Parametri, impostati dall'utente | Impostato sul Server | | |
|---|---|---|---|
| | Deve | Può | Non può |
| Installare | + | + | |
| Non installare | + | | |

3. Premere sul tasto **Salva** per salvare le impostazioni e apportare le modifiche corrispondenti nel pacchetto antivirus di workstation.



Componente **Anti-spam VadeRetro** non può essere installato, se non è installato almento uno dei seguenti prodotti:

- **SpIDer Mail**,
- **Dr.Web plug-in per MS Outlook**,
- **Dr.Web per IBM Lotus Domino**,
- **Dr.Web per MS Exchange Server**,
- **Dr.Web per Qbik WinGate plug-in**.

## 7.3. Configurazione di Dr.Web Enterprise Agent per il SO Windows®

***Per visualizzare o modificare le impostazioni di Dr.Web Enterprise Agent su workstation con il SO Windows:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**.
2. Nella finestra aperta nella lista gerarchica premere su nome

workstation o gruppo.

3. Nel menu di gestione aperto (pannello a sinistra) scegliere la voce **Dr.Web Enterprise Agent per Windows**.
4. Si apre la finestra di impostazioni di **Agent**.



Se si apportano delle modifiche in queste impostazioni, non accordate con le impostazioni del **Server** (in particolare, modifica di modalità di codifica e di compressione, nonché della chiave di codifica), questo comporta perdita di connessione tra **Agent** e **Server**.

5. Apportate delle modifiche nelle impostazioni di **Agent** via il **Centro gestione**, per accettare tali modifiche, premere sul tasto **Salvare**.

## *Scheda Generale*

Nella scheda **Generale** si indicano i parametri generali di **Agent**:

- Nel campo **Chiave aperta del server** indicare il percorso alla chiave di codifica aperta di **Enterprise Server** sul computer dell'utente.
- Nel campo **File della chiave locale di Dr.Web** indicare il percorso al file della chiave di licenza del prodotto di Dr.Web per conservare il file anche su workstation. Nel caso contrario, il file della chiave si troverà solamente sul **Server**.
- Nel campo **Periodicità invio statistiche (min.)** inserire l'intervallo di tempo in minuti per l'invio di Agent al Server di tutte le informazioni statistiche, raccolte su workstation.
- Nella lista a cascata **Lingua** impostare la lingua dell'interfaccia di **Agent** e dei componenti di **Dr.Web Anti-virus** su workstation o su gruppo di workstation con il SO Windows.
- Mettere il flag **Microsoft Network Access Protection** per attivare il supporto di tecnologia Microsoft® Network Access Protection, utilizzata per il monitoraggio dello stato di workstation (per più informazioni v. NAP Validator).
- Mettere il flag **Sincronizzare ora** per attivare la sincronizzazione di ora di sistema del computer con **Agent** con

ora del computer con **Dr.Web ESS Server**.

- Flag **Bloccare modifica file di sistema HOSTS** mette il blocco su introduzione delle modifiche nel file HOSTS, utilizzato dal sistema operativo per semplificare l'accesso a Internet: per trascodificare i nomi testuali di alcuni siti in indirizzi IP corrispondenti. Modifica del file HOSTS potrebbe costatare le attività dei programmi nocivi.
- Flag **Bloccare modifica oggetti critici Windows** pone il blocco di modifica di oggetti critici del sistema operativo (registro ecc).

## *Scheda Rete*

Nella scheda **Rete** si trovano i parametri, che definiscono le configurazioni di comunicazione con il **Server**:

- Nel campo **Server** si imposta l'indirizzo di **Enterprise Server.** Questo campo può rimanere vuoto. In questo caso **Agent** utilizza come indirizzo di **Enterprise Server** il valore del parametro, indicato nelle configurazioni del computer locale dell'utente (indirizzo del **Server**, da cui è stata eseguita l'installazione).

  È possibile impostare un indirizzo di **Server** o più indirizzi di diversi **Server**. Per aggiungere un altro indirizzo di **Server**, premere sul tasto  e inserire l'indirizzo nel campo che è stato aggiunto. Il formato in cui si devono impostare indirizzi di rete di **Server** è descritto nell'Allegato E. Specifica indirizzo di rete.

  Esempio di come si può impostare l'indirizzo di **Server**:

  tcp/10.4.0.18:2193
  tcp/10.4.0.19
  10.4.0.20



Quando più indirizzi vengono impostati su **Agent**, gli indirizzi di **Server** si scrivono con uno spazio nel campo **Server** della sezione **Impostazioni → Connessione** a cui si accede tramite il menu contestuale dell'icona di **Agent**.



Se si imposta il valore non corretto/non valido del parametro **Server**, **Agent** si disconnettono dal **Server** e non possono più connettersi ad esso. In questo caso l'impostazione dell'indirizzo del **Server** si deve eseguire direttamente su workstation.

- Nel campo **Iterazioni ricerca** impostare il parametro, che definisce il numero di tentativi di ricerca di **Dr.Web Enterprise Server** durante la connessione nella modalità Mulicasting.
- Nel campo **Timeout ricerca (sec)** impostare il periodo fra i tentativi di ricerca di **Enterprise Server** in secondi durante la connessione nella modalità Mulicasting.
- Campi **Modalità compressione** e **Modalità codifica** definiscono le impostazioni corrispondenti della compressione e della codifica del traffico di rete (v. anche Utilizzo codifica e compressione traffico).
- Nel campo **Ascoltare scansione rete** indicare la porta UDP, utilizzata dal **Centro gestione** per la ricerca in rete di **Enterprise Agent** operativi. Per bloccare l'ascolto delle porte, impostare il valore **NONE**.

  Il parametro viene impostato nel formato dell'indirizzo di rete, riportato in Allegato E. Specifica indirizzo di rete.

  Di default si utilizza **udp/:2193**, il che significa "tutte le interfacce, porta 2193".

## *Scheda Mobilità*

Nella scheda **Mobilità** si impostano i parametri di *Modalità mobile* di **Agent**:

- Nel campo **Periodicità aggiornamenti (sec)** indicare l'intervallo di tempo tra aggiornamenti del software antivirus in secondi.
- Mettere il flag **Verificare connessione Internet** per attivare la verifica della connessione a Internet prima di iniziare il processo di aggiornamento.
- Mettere il flag **Utilizzare server proxy** per utilizzare HTTP del server proxy alla ricezione di aggiornamenti da Internet. In questo caso diventano attivi i campi di impostazioni del server proxy utilizzato.

## *Scheda log*

Nella scheda **Log** si impostano i parametri di gestione del log di **Agent:**

- Nel campo **File del log** si imposta il percorso al file di log e il suo nome sul computer dell'utente.
- Il parametro **Livello del log** definisce il livello di dettagli nella gestione del log (v. anche Gestione del log del server).
- I flag: **Limitazione dimensione file del log, Comprimere i file vecchi** e i campi: **Conservare al massimo** <…> **file di dimensione** <…> definiscono tali parametri del logging, come: numero e dimensione dei file di log, nonché la necessità di comprimere i file vecchi.
- Parametro **Numero file log aggiornamento** definisce il numero massimo dei file del log di aggiornamento.

## *Scheda Interfaccia*

Nella scheda **Interfaccia** si impostano le opzioni di interfaccia di **Enterprise Agent**.

Nel campo **Differimento del messaggio di benvenuto** specificare il tempo in minuti per il quale si differisce la visualizzazione del messaggio di benvenuto dopo l'avvio dell'interfaccia di **Agent**. Mettere il parametro in valore **-1** per disabilitare la visualizzazione del messaggio di benvenuto. Il messaggio di benvenuto viene messo sullo

schermo in una finestra pop-up che contiene il nome del prodotto **Dr.Web**, la sua versione e le informazioni sul diritto di autore.

Nella scheda **Interfaccia** si può marcare il tipo di avvisi di eventi, che riceve l'utente. Per farlo, mettere il flag corrispondente:

- **Avvisi critici -** ricevere solamente avvisi critici. Sono avvisi periodici:
  - di errore di aggiornamento del software antivirus o di un suo componente;
  - di necessità di riavviare il computer dopo l'aggiornamento.

  L'avviso viene visualizzato solamente se l'utente ha i diritti dell'amministratore.
- **Avvisi dei virus** - ricevere solamente gli avvisi dei virus. Sono gli avvisi di rilevamento di un virus (dei virus) da uno dei componenti del software antivirus.
- **Avvisi importanti** - ricevere solamente avvisi importanti. Sono avvisi:
  - di errori durante l'avvio di un componente del software antivirus;
  - di errori di aggiornamento del software antivirus o di un suo componente, viene visualizzato appena la procedura di aggiornamento va in errore;
  - di necessità di riavviare il computer dopo l'aggiornamento, viene visualizzato subito dopo l'aggiornamento;
  - di necessità di aspettare l'avviso di richiesta di riavvio per completare l'installazione dei componenti.
- **Avvisi poco importanti** - ricevere solamente avvisi poco importanti. Sono avvisi:
  - di avvio della scansione remota;
  - di completamento della scansione remota;
  - di avvio di aggiornamento del software antivirus o di un suo componente;
  - di completamento con successo dell'aggiornamento del software antivirus o di un suo componente (senza la necessità di riavvio).

Per farsì che l'utente riceva tutti i gruppi di messaggi, mettere tutti i quattro flag. Altrimenti saranno visualizzati solo i messaggi di gruppi indicati.



L'utente può gestire ricezione di avvisi, oltre **Avvisi critici**, la cui ricezione è configurata solamente per l'amministratore.

# 7.4. Configurazione orario processi su workstation

*Orario* è la lista delle azioni, eseguite automaticamente nelle ore programmate su workstation. Applicazione principale di orari – eseguire la scansione di workstation per virus nel tempo più comodo per gli utenti senza dover avviare lo **Scanner** manualmente. Oltre questo, **Enterprise Agent** permette di eseguire altri tipi di azioni, descritti sotto.

Ci sono due tipi di orari:

- *Orario centralizzato*. Orario, impostato dall'amministratore di rete antivirus e aderente a tutte le regole di ereditarietà delle configurazioni.
- *Orario locale di workstation*. Orario, impostato dall'utente su workstation concreta (se tale workstation ha i diritti), conservato localmente su tale workstation; tale orario non è un oggetto, gestito da **Enterprise Server**.

## Orario centralizzato

Modifica dell'orario centralizzato di esecuzione regolare dei processi di una workstation concreta (e anche di gruppi) è eseguita con il **Centro gestione**.

***Alla modifica di orario centralizzato eseguire le seguenti azioni:***

1. Per aprire la finestra di modifica dell'orario scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo. Nel menu di gestione aperto (pannello a sinistra) scegliere la voce **Orario**.
2. Si possono eliminare i processi attuali, aggiungere nuovi o modificare esistenti. Si può bloccare esecuzione del processo o consentire esecuzione del processo bloccato in precedenza. Tale azione è descritta di seguito in dettagli.

   Di default per le workstation sotto la gestione del SO Windows e del SO Windows Mobile orario contiene 2 processi:

   - **Startup scan** - scansione di workstation all'avvio (consentita),
   - **Daily scan** - scansione di workstation quotidiana (bloccata).
3. Alla fine di modifica dell'orario premere sul tasto **Salva** per accettare le modifiche.



Se alla fine di modifica viene creato l'orario vuoto (che non ha processi), **Centro gestione** propone di utilizzare orario ereditato dai gruppi o di utilizzare l'orario vuoto. L'orario vuoto deve essere impostato per rifiutare all'orario, ereditato dai gruppi.

***Per aggiungere un processo nuovo:***

1. Per creare un nuovo processo premere sul tasto  **Nuovo processo** nella barra degli strumenti del **Centro gestione**.



I valori dei campi, marcati con il carattere *, sono obbligatori da impostare.

2. Nella scheda **Generale** impostare i seguenti parametri:

- Inserire nel campo **Nome** il nome del processo, con il quale esso verrà visualizzato nell'orario.
- Per attivare l'esecuzione del processo, mettere il flag **Permettere l'esecuzione**.

Se il flag non è posto, il processo sarà presente nella lista, ma non verrà eseguito.

- Il flag posto su **Processo critico** fa eseguire il processo all'avvio successivo di **Enterprise Agent**, se l'esecuzione di tale compito viene saltata (**Enterprise Agent** è disattivato al momento di esecuzione del processo). Se in un certo periodo il processo viene saltato più volte, all'avvio di **Enterprise Agent** viene eseguito 1 volta.



Se all'avvio di workstation si devono eseguire più processi di scansione con lo stesso scanner (**Scanner per Windows** o **Enterprise Scanner**), ne viene eseguito solamente uno – il primo nella coda.

Per esempio, se è consentito il processo **Startup scan** (scansione di workstation all'avvio) ed è stata posposta la scansione con **Enterprise Scanner**, all'avvio di workstation verrà eseguito **Startup scan**, e la scansione critica posposta non potrà essere eseguita.

3. Nella scheda **Azione** scegliere dalla lista a cascata **Azione** il tipo di processo. Dopo la scelta fatta la parte inferiore della finestra sarà diversa per varie alternative.
   - Se è scelto **Avvio**, inserire nel campo **Percorso** il nome completo (con il percorso) del file eseguibile, che è da avviare, e nel campo **Argomenti** - parametri di riga di comando per il programma avviato.
   - Se è scelto **Dr.Web Scanner per Windows** o **Dr.Web Enterprise Scanner per Windows**, si apre la finestra di configurazione di scansione, descritta in Avvio e arresto di scanner antivirus su workstation.
   - Se è scelto **Logging**, inserire nel campo **Riga** il testo del messaggio, scritto nel log.
4. Nella scheda **Ora** configurare l'ora di avvio del processo.

   Per farlo, prima di tutto scegliere nella lista a cascata

**Periodicità** una delle modalità di avvio:

- Giornaliero,
- Iniziale,
- Mensile,
- Ogni ora,
- Ogni X minuti,
- Settimanale.

La descrizione dei parametri di ogni modalità è riportata nella tabella 7-2.

5. Al completamento di inserimento di parametri di processo premere sul tasto **Salva**.

**Tabella 7-2. Modalità di avvio e loro parametri**

| Modalità di avvio | Parametri e descrizione |
|---|---|
| Giornaliero | Si devono inserire l'ora e il minuto - il processo viene avviato giornalmente nell'ora indicata. |
| Iniziale | Si deve scegliere il giorno (il giorno del mese), inserire l'ora e il minuto - il processo viene avviato nel giorno impostato del mese nell'ora indicata. |
| Mensile | Si deve scegliere il giorno della settimana, inserire l'ora e il minuto - il processo viene avviato nel giorno della settimana impostato e nell'ora indicata. |
| Ogni ora | Si deve inserire il numero da 0 a 59, che imposta il minuto di ogni ora, in cui viene avviato il processo. |
| Alla terminazione | I parametri supplementari non sono richiesti. Il processo viene avviato alla terminazione dell'operazione di**Agent**.<br>Il processo di terminazione per **Dr.Web Enterprise Scanner** e **Dr.Web Scanner per Windows** non viene eseguito. |
| Ogni X minuti | Si deve inserire il valore **X**.<br>Con **X** pari a `60` o superiore il processo viene avviato ogni **X** minuti. Con **X** minore a `60` il processo viene avviato ogni minuto dell'ora, multiplo di **X**. |

| Modalità di avvio | Parametri e descrizione |
|---|---|
| Settimanale | I parametri supplementari non sono richiesti. Il processo viene avviato all'inizio di operazione di **Agent**. |

***Per modificare il processo attuale:*** scegliere il processo dalla lista, premendo su di esso con il tasto sinistro del mouse. Le azioni successive sono analoghe all'inserimento di un processo nuovo (v. sopra).

***Per eliminare un processo:***

1. Mettere il flag accanto al processo.
2. Premere sul tasto  **Rimuovi queste impostazioni** nella barra degli strumenti del **Centro gestione**.

## Orario locale

***Per modificare orario locale di workstation:***

1. Nel menu contestuale di **Agent** nella voce **Orario** scegliere la variante **Locale**.
2. Si apre la finestra di modifica dell'orario locale di **Enterprise Agent**.



Nel menu contestuale di **Agent** nella voce **Orario**, la variante **Locale** sarà disponibile solo nel caso se alla modifica dei diritti della workstation antivirale è stato posto il flag **Creazione orario locale**.

Utilizzando l'orario locale, l'utente può avviare scansione con configurazione dei parametri. Le varianti di impostazione di oggetti da scansionare, le chiavi della riga di comando che definiscono parametri del programma, nonché i parametri della riga di comando per **Scanner** sono descritti nel manuale **Dr.Web® Anti-virus per Windows. Manuale dell'utente.**

3. Alla fine di modifica premere sulla voce **Chiudere**.



Con le configurazioni di workstation predefinite, cioè senza alcun intervento dell'amministratore di rete antivirus, su workstation è operativo il monitoraggio antivirus ed inoltre vengono periodicamente avviati i processi di aggiornamento del software e la scansione antivirus.

# 7.5. Scansione antivirus di workstation



L'utente di workstation può eseguire la scansione antivirus di workstation autonomamente, utilizzando il componente **Dr.Web Scanner per Windows**. L'icona per avviare questo componente viene messa all'installazione del software antivirus su desktop. Avvio e operazione con successo di **Scanner** sono possibili anche in caso in cui **Agent** non sia operativo, compreso l'avvio del SO Windows nella modalità provvisoria.

***Per ogni workstation si può:***

- Visualizzare la lista di tutti i componenti antivirus avviati al momento.
- Arrestare per tipi i componenti antivirus avviati.
- Avviare i processi di scansione antivirus con la configurazione dei parametri di scansione. Le scansioni possono essere avviate per:
  - **Dr.Web Scanner per Windows**,
  - **Dr.Web Enterprise Scanner per Windows**,
  - **Dr.Web Enterprise Scanner per Unix**,
  - **Dr.Web Enterprise Scanner per Mac OS X**.

### 7.5.1. Visualizzazione e arresto del funzionamento di componenti avviati

***Per visualizzare la lista e per il completamento del funzionamento dei componenti avviati:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere sul nome workstation o gruppo. Nel menu di gestione aperto (pannello a sinistra) scegliere la voce **Componenti avviati**.

   Si apre la lista di tutti i componenti attualmente attivi, sia avviati manualmente da Lei o dall'utente, sia avviati nel modo programmato.

2. Se è necessario arrestare uno dei componenti, mettere il flag accanto a questo componente, dopodiché nella barra degli strumenti premere sul tasto **Interrompi**. Il componente viene arrestato e eliminato dalla lista.

### 7.5.2. Arresto funzionamento componenti avviati per tipi



Con utilizzo di questa opzione vengono arrestate le scansioni in corso e i monitoraggi avviati, escluso **SpIDer Guard**.

Attenzione! Avvio di monitoraggi **SpIDer Mail** e **SpIDer Gate** dal **Centro gestione** non è disponibile.

Si possono arrestare i componenti su workstation:

- avviati dall'amministratore manualmente,
- avviati dall'utente,
- avviati nel modo programmato secondo l'orario.

Si possono simultaneamente arrestare tutti i componenti eseguibili, che soddisfano un certo criterio. È soprattutto comodo, se tale comando viene dato subito a più workstation.

***Per arrestare tutti i componenti eseguibili del certo tipo:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica scegliere il gruppo necessario o le workstation antivirus singoli.
2. Nella barra degli strumenti della cartella della rete antivirus premere su **Gestione dei componenti**. Nella lista a cascata scegliere la voce **Interrompere quelli avviati**. Si apre la finestra di configurazione del tipo dei componenti arrestati.
3. Mettere i flag accanto ai nomi dei tipi di componenti da arrestare immediatamente oppure accanto all'intestazione dell'area **Interruzione dei componenti avviati** – per scegliere tutti i processi della lista.
4. Premere sul tasto **Interrompere**.

## 7.5.3. Avvio scansione workstation

***Per avviare il processo di scansione:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**.
2. Nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo.
3. Nella barra degli strumenti premere sulla voce **Scansionare**.
4. Nella lista aperta nella barra degli strumenti scegliere una delle modalità di scansione:

   **Dr.Web Scanner per Windows. Scansione rapida**. In questa modalità viene eseguita la scansione dei seguenti oggetti:

   - memoria operativa,

- settori di avvio di tutti i dischi,
- oggetti di auto-esecuzione,
- cartella radice del disco di avvio,
- cartella radice del disco di installazione del SO Windows,
- cartella di sistema del SO Windows,
- cartella `Miei documenti`,
- cartella temporanea del sistema,
- cartella temporanea dell'utente.

Alla scelta di questa voce inizia la scansione per virus con i parametri di **Scanner** predefiniti.

 **Dr.Web Scanner per Windows. Scansione completa**. In questa modalità viene eseguita la scansione completa di tutti i dischi rigidi e di tutti i dispositivi rimovibili (compresi i settori di avvio). Alla scelta di questa voce inizia la scansione con i parametri di **Scanner** predefiniti.

 **Dr.Web Scanner per Windows. Scansione personalizzata**. Questa modalità permette di scegliere qualsiasi cartella o file per la scansione successiva. Alla scelta di questa voce si apre la finestra di configurazione di **Scanner**. Impostare i parametri di scansione e gli oggetti scansionati del file system (queste azioni sono descritte sotto in dettagli) e premere sul tasto **Controlla per i virus**.

 **Dr.Web Enterprise Scanner per Windows**. In questa modalità viene eseguita la scansione personalizzata con **Dr.Web Enterprise Scanner**. A scelta di tale voce si apre la finestra di configurazione di **Scanner**. Impostare i parametri di scansione e i contenuti di oggetti controllati del file system (queste azioni sono descritte sotto in dettagli) e premere sul tasto **Controlla per i virus**.

 **Dr.Web Enterprise Scanner per Unix**. Per scansionare le workstation, che operano sotto la gestione del SO della famiglia UNIX. Impostare i parametri di scansione e gli oggetti controllati del file system e premere sul tasto **Controlla per i**

**virus**.

 **Dr.Web Enterprise Scanner per Mac OS X**. Per scansionare le workstation, che operano con il SO della famiglia Mac OS X. Impostare i parametri di scansione e gli oggetti controllati del file system e premere sul tasto **Controlla per i virus**.

## 7.5.4. Configurazione parametri Scanner per SO Windows®

***Per visualizzare e modificare i parametri di Scanner sono disponibili più varianti:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo. Nel menu di gestione aperto (pannello a sinistra) scegliere la voce **Dr.Web Scanner per Windows**. Si apre la finestra delle configurazioni di **Scanner**. Tale lista dei parametri è la più completa e include tutti i gruppi dei parametri, descritti sotto.
2. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo. Nella barra degli strumenti premere sulla voce  **Scansionare**. Nella lista aperta nella barra degli strumenti scegliere la voce  **Dr.Web Scanner per Windows. Scansione personalizzata**. Nel pannello a destra si apre la finestra delle configurazioni di **Scanner**. Tale lista di parametri è una lista abbreviata e permette di impostare solo i parametri principali, che rientrano nei gruppi delle configurazioni **Generali**, **Azioni**, **Report** e **Altro**.

3. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo. Nella barra degli strumenti premere sulla voce **Scansionare**. Nella lista aperta nella barra degli strumenti scegliere la voce **Dr.Web Enterprise Scanner per Windows**. Nel pannello a destra si apre la finestra delle configurazioni di **Scanner**. Tale lista dei parametri permette di impostare solamente i parametri principali per **Enterprise Scanner**, che fanno parte del gruppo delle configurazioni **Generali, Azioni** e **Percorsi esclusi**.

## Generali

- Flag **Analisi eurisica** è attivato di default; in questo caso **Scanner** cerca di rilevare i virus sconosciuti con analisi eurisitica. In questa modalità possono esserci dei falsi positivi di **Scanner**.
- Flag **Controllo di archivi** è attivato di default. Prescrive a **Scanner** di cercare i virus nei file, compressi in archivi di file.
- Flag **Controllo di file di posta** è attivato di default. Prescrive di scansionare le caselle di posta.
- Flag **Controllo dei moduli e processi in execuzione (Scansione memoria** per **Enterprise Scanner**) è attivato di default. Prescrive di scansionare i processi, avviati nella memoria operativa.
- Flag **Controllo dei programmi avviati automaticamente** è attivato di default. Prescrive di scansionare i file, avviati automaticamente all'avvio del sistema operativo.
- Flag **Controllo dei settori di avvio** è attivato di default. Prescrive a **Scanner** la scansione dei settori di avvio. Vengono scansionati sia i settori di avvio dei dischi logici, sia i settori di avvio principali dei dischi fisici.
- Flag **Controllo di sottocartelle** (assente per **Enterprise Scanner**) è attivato di default. Viene utilizzato all'impostazione del percorso di scansione e prescrive a Scanner di controllare non solamente i file, ma anche tutte le sottocartelle innestate al percorso impostato.

***All'impostazione di configurazioni di Scanner via la voce del menu di gestione Dr.Web Scanner per Windows sono disponibili i seguenti parametri:***

- Flag **Controllare il file HOSTS** prescrive il controllo dello stato del file di sistema HOSTS, che viene utilizzato dal sistema operativo per semplificare l'accesso alla rete Internet: per trasformare i nomi testuali di alcuni siti in indirizzi IP corrispondenti. Modifica del file HOSTS potrebbe costatare le attività dei programmi nocivi.
- La voce **Scansionare** definisce la modalità di scansione. Nella lista a cascata scegliere una delle varianti:
  - **Tutti i file** – per scansionare tutti i file, nonostante il nome e l'estensione.
  - **Secondo la maschera** – per scansionare solo i file, i cui nomi e estensioni fanno parte della lista, impostata nella sezione **Lista maschere**.
  - **Tipi enumerati** – per scansionare solo i file, cui estensioni fanno parte della lista, impostata nella sezione **Lista estensioni**.
- Flag **Conferma di un'azioni** prescrive l'invio all'utente di avvisi di eventi e di richieste di conferma delle azioni di **Scanner**.
- Flag **Richiesta di controllo del dischetto successivo** viene utilizzato durante la scansione di dispositivi rimovibili (dischi magnetici (floppy), dischi CD/DVD, schede flash) e prescrive di visualizzare una richiesta di connessione del dispositivo (cambio di quello attuale) e della scansione del dispositivo successivo.

***Impostando le configurazioni di Scanner e richiamandolo nella barra degli strumenti, scegliere una delle due modalità alternative:***

1. **Scansionare tutti i dischi**.

   per **Enterprise Scanner** nella variante **Scansionare tutti i dischi** impostare, quali dei dischi del sistema devono essere scansionati:

   - mettere il flag **Dischi locali** per la scansione di tutti i dischi fissi (disco rigido ecc);

- mettere il flag **Dischi ti rimovibili** per la scansione di tutti i dispositivi rimovibili come: dischi magnetici (floppy), dischi CD/DVD, schede flash ecc.

In questa modalità può inoltre essere impostata la lista **Percorsi esclusi** (il modo di impostarli è descritto di seguito).

2. **Scansionare i percorsi indicati**.

   Nella variante **Scansionare i percorsi indicati** impostare la lista di percorsi scansionati (il modo di impostarli è descritto di seguito).

***Per Enterprise Scanner per Windows sono inoltre disponibili i seguenti flag:***

- Flag **Tecnologia BurstScan** prescrive di utilizzare tale tecnologia, che accelera notevolmente la scansione nei sistemi moderni, che hanno processori multicore.
- Flag predefinito **Scansione a bassa priorità** permette di diminuire il carico di **Scanner** sulle risorse del computer a disposizione. In questo caso altri processi possono avere la priorità più alta di esecuzione che nel caso di configurazione disattivata. Questo è raggiunto per via di modifica dinamica delle priorità di flussi di scansione.
- Flag **Controllo dei container** prescrive allo **Scanner** di controllare i contenitori di file di vari tipi.
- Lista **Azioni dopo la scansione** prescrive esecuzione automatica di azione impostata subito dopo la fine del processo di scansione: spegnere, riavviare, far passare alla modalità corrispondente o non applicare nessuna azione al computer dell'utente.
- Flag **Scollegare la rete per il tempo di scansione** permette di disconnettere il computer dalla rete locale e da Internet per il periodo della scansione.

Nella sezione **Limitazioni** sono disponibili le seguenti configurazioni:

- **Tempo massimo di scansione (ms)** – tempo massimo in millisecondi, durante il quale l'oggetto viene scansionato. Alla scadenza del periodo indicato la scansione dell'oggetto viene sospesa.

- **Profondità massima di annidamento di un archivio (KB)** - se il livello di innestazione dell'archivio supera l'indicato, la scansione viene eseguita sono fino al livello indicato di innestazione.
- **Dimensione massima di un archivio (KB)** - se la dimensione dell'archivio supera la dimensione indicata, la decompressione e la scansione non vengono eseguite.
- **Grado massimo di compressione** - se lo **Scanner** definisce che il coefficiente di compressione dell'archivio supera quello indicato, la decompressione e la scansione non vengono eseguite.
- **Dimensione massima di un oggetto spacchettato (KB)** - se lo **Scanner** definisce che dopo la decompressione l'archivio supera la dimensione indicata (in kB), la decompressione e la scansione non vengono eseguite.
- **Soglia di controllo del grado di compressione (KB)** - dimensione minima del file all'interno dell'archivio, partendo dalla quale si esegue il controllo del coefficiente di compressione.

## Azioni

Nel gruppo di parametri **Azioni** si imposta la reazione di **Antivirus** al rilevamento di file infetti o sospetti, programmi nocivi e archivi infetti.

Sono previste le seguenti azioni per oggetti rilevati:

- **Curare** - ripristinare lo stato di oggetto infetto prima di infezione. Se non è possibile curarlo, si applica la configurazione, impostata per oggetti incurabili.

  Questa azione è disponibile solo per oggetti, contaggiati da un virus noto incurabile, esclusi i trojan e i file infetti all'interno di oggetti composti (archivi, file di posta elettronica o contenitori dei file).

- **Rimuovere** – eliminare oggetti contaggiati.
- **In quarantena** – mettere oggetti contaggiati nella cartella di **Quarantena**.
- **Rinominare** – rinominare oggetti contaggiati a seconda della

regola, impostata nel campo **Template per rinominare file**.

- **Informare** – limitarsi all'avviso sul rilevamento del virus (su configurazione della modalità di avviso v. Configurazione avvisi).
- **Ignorare** – saltare l'oggetto, non eseguendo qualsiasi azione e non avvisandone.

**Tabella 7-3. Azioni di Scanner su oggetti nocivi rilevati**

| Azione | Oggetto | | | | |
|---|---|---|---|---|---|
| | Adware | Contenitori infetti | Infetti | Sospetti | Incurabili |
| Curare | | | +/* | | |
| Rimuovere | + | + | + | + | + |
| In quarantena | + | +/* | + | + | +/* |
| Rinominare | + | + | + | + | + |
| Informare | +/* | + | + | +/* | + |
| Ignorare | + | | | | |

**Segni convenzionali**

| | |
|---|---|
| + | azione consentita per questo tipo di oggetti |
| +/* | azione predefinita per questo tipo di oggetti |

***Per impostare le azioni da applicare a oggetti nocivi rilevati si utilizzano le seguenti configurazioni:***

- Nel campo **Template per rinominare file** si indica la maschera di estensione, che ricevono oggetti rinominati, se per essi è stata indicata l'azione **Rinominare** al rilevamento. Di default si propone la variante `#??`, cioè il primo carattere di estensione viene sostituito con il carattere `#`. Questa maschera può essere modificata, ma come sostituzione non si devono applicare le estensioni standard (`EXE`, `COM`, `BAT`, `DOC`, `PAS`, `BAS` ecc).
- Lista a cascata **Adware** imposta la reazione di **Scanner** al rilevamento di questa tipologia del software indesiderabile.



Durante l'impostazione di azione **Ignorare** per Adware non si applica nessuna azione: all'utente non se ne visualizza nessun avviso, al contrario del caso di opzione attiva **Informare** al rilevamento di virus.

- Nello stesso modo alle azioni applicate ad Adware, si imposta la reazione di **Scanner** al rilevamento di altro software indesiderabile, come:
  - Dialer;
  - Joke;
  - Riskware;
  - Hacktool.
- Lista a cascata **Riavviare il computer** imposta la modalità di riavvio del computer al completamento della scansione.
- Lista a cascata **Container infetti** imposta la reazione di **Scanner** al rilevamento di file infetto o sospetto, contenuto in file di archivio o in contenitore. La reazione si imposta per tutto l'archivio intero.
- Lista a cascata **Infetti** imposta la reazione di **Scanner** al rilevamento del file, contaggiato con un virus conosciuto.
- Lista a cascata **Sospetti** imposta la reazione di **Scanner** al rilevamento del file, presumibilmente contaggiato con virus (scatto di analisi euristica).



Durante la scansione, che comprende la cartella di installazione del SO, si consiglia di scegliere per tutti i file sospetti la reazione **Informare**.

- Lista a cascata **Incurabili** imposta la reazione di **Scanner** al rilevamento del file, contaggiato da un virus conosciuto incurabile (e quando il tentativo di cura intrapreso non è riuscito).

- Il flag **Consentire di rimuovere archivi** permette di eliminare archivi e file di posta infetti rilevati. Se tale flag è posto, nelle sezioni **Archivi infetti** e **File di posta infetti**, locati di seguito, è presente la variante di azione **Rimuovere**. Se si toglie tale flag, si ammettono solo le azioni **In quarantena** (predefinita per archivi), **Rinominare** e **Informare** (predefinita per file di posta).

## Percorsi da escludere e File da escludere

***Durante la modifica di liste dei percorsi e file esclusi:***

- Inserire il percorso o il file richiesto nella riga **Percorsi da escludere** o **File da escludere** rispettivamente.
- Per aggiungere una nuova riga alla lista, premere sul tasto  e nella riga aperta inserire il percorso richiesto.
- Per eliminare un elemento dalla lista, premere sul tasto  accanto alla riga corrispondente.

***Lista di oggetti esclusi può contenere elementi di seguenti tipi:***

1. Percorso diritto nel formato esplicito fino a oggetto escluso. In questo caso:
   - Carattere \ o / – esclusione dalla scansione di tutto il disco, su cui si trova la cartella di installazione del SO Windows,
   - Percorso, che finisce con il carattere \ – questa cartella si esclude dalla scansione,
   - Percorso, che non finisce con il carattere \ – qualsiasi sottocartella, il percorso alla quale inizia con la riga indicata, si esclude dalla scansione.

   **Per esempio**: `C:\Windows` - non scansionare i file della cartella `C:\Windows` e tutte le sue sottocartelle.

2. Le maschere di oggetti, esclusi dalla scansione. Per impostare le maschere si possono utilizzare i caratteri `?` e `*`.

**Per esempio**: `C:\Windows\*\*.dll` - non scansionare tutti i file con estensione `dll`, locati in tutte le sottocartelle della cartella `C:\Windows`.

3. Espressione regolare. I percorsi si possono impostare con le espressioni regolari. Inoltre qualsiasi file, il cui nome completo (con il percorso) corrisponde a una espressione regolare, si esclude dalla scansione.



Prima di avviare il processo di scansione per virus prendere conoscenza dei consigli di utilizzo dei programmi antivirus per computer con il SO Windows Server 2003, il SO Windows 2000 e il SO Windows XP. L'articolo che contiene le informazioni necessarie si trova all'indirizzo - http://support.microsoft.com/kb/822158/it. Materiale di questo articolo è volto ad ottimizzare il rendimento del sistema.

Sintassi di espressioni regolari, utilizzate per definire percorsi esclusi, è il seguente:

```
qr{espressione}flag
```

Di solito come flag si utilizza il carattere `i`, questo flag significa "non prendere in considerazione differenza di lettere maiuscole/minuscole".

***Esempi di definizione di percorsi e di file esclusi con espressioni regolari sono riportati sotto:***

- `qr{\\pagefile\.sys$}i` — non scansionare i file di swap del SO Windows NT,
- `qr{\\notepad\.exe$}i` — non scansionare i file `notepad.exe`,
- `qr{^C:}i` — non scansionare proprio niente sul disco `C`,
- `qr{^.:\\WINNT\\}i` — non scansionare niente nelle cartelle `WINNT` su tutti i dischi,
- `qr{(^C:)|(^.:\\WINNT\\)}i` — unione di due casi precedenti,
- `qr{^C:\\dir1\\dir2\\file\.ext$}i` — non scansionare il file `c:\dir1\dir2\file.ext`,

- `qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i` — non scansionare il file `file.ext`, se è nella cartella `c:\dir1\dir2` e nelle sue sottocartelle,
- `qr{^C:\\dir1\dir2\\}i` — non scansionare la cartella `c:\dir1\dir2` e le sue sottocartelle,
- `qr{dir\\[^\\]+}i` — non scansionare la sottocartella `dir`, che si trova in qualsiasi cartella, ma scansionare le sottocartelle,
- `qr{dir\\}i` — non scansionare la sottocartella `dir`, che si trova in qualsiasi cartella, e le sue sottocartelle.

Utilizzo di espressioni regolari è brevemente descritto in Allegato K.

Per i link alle descrizioni complete di sintassi di espressioni regolari v. Link.

## Lista di estensioni (richiamando configurazioni via il menu di gestione)

La sezione **Lista di estensioni** è attiva solo se nella sezione **Generali** nella voce **Scansionare** è impostata la variante **Tipi enumerati**. In questo caso vengono scansionati solo i file, le cui estensioni rientrano in questa lista.

Modificando la lista di estensioni, utilizzare il tasto  per aggiungere elementi nuovi alla lista, il tasto  - per eliminare elementi della lista a disposizione.

In elementi di lista di estensioni si possono utilizzare i caratteri speciali `*` e `?`. Di default si conserva la lista dei file eseguibili e file di archivio. Per ripristinare la lista predefinita utilizzare il tasto  .

## Lista di maschere (richiamando configurazioni via il menu di gestione)

La sezione **Lista di maschere** è attiva solo se nella sezione **Generali** nella voce **Scansionare** è impostata la variante **Secondo la maschera**. In questo caso vengono scansionati solo i file, i cui nomi e estensioni rientrano in questa lista.

Modificando la lista di maschere, utilizzare il tasto  per aggiungere elementi nuovi alla lista, il tasto  - per eliminare elementi della lista a disposizione.

In elementi di lista di estensioni si possono utilizzare i caratteri speciali `*` e `?`. Di default si conserva la lista dei file eseguibili e file di archivio. Per ripristinare la lista predefinita utilizzare il tasto  .

## Altro (oltre Enterprise Scanner)

Nella sezione **Altro** si indicano i parametri aggiuntivi di **Scanner**:

- Flag **Usare il disco per creare il file dello swap** prescrive utilizzo del disco rigido per creare file di swap per evitare che manchi la memoria operativa, utilizzata da **Scanner** durante la scansione di grandi volumi dei dati (grandi archivi ecc).
- Flag **Ripristinare la data di accesso** prescrive di ripristinare dopo la scansione la data di ultimo accesso al file (sostituire con la data precedente alla scansione).
- Flag **Salvare impostazioni automaticamente** prescrive di salvare automaticamente le configurazioni di **Scanner** dopo il completamento della sessione attuale di operazione.
- Nella lista **Priorità di scansione** si imposta la priorità dei flussi del processo di scansione. Scegliere una delle varianti proposte:
  - **inuttilizzata** - non si consiglia di impostare questo livello di priorità per evitare il rallentamento di operazione di **Scanner** e, quindi, un notevole aumento del tempo di scansione,

- **bassa**,
- **più bassa del normale**,
- **normale** - priorità scansione consigliata,
- **più alta del normale**,
- **alta**,
- **time-critical** - non si consiglia di impostare questo livello di priorità per evitare che lo **Scanner** crei un forte carico sul sistema operativo durante la scansione.

### Report

Nella sezione **Report** si può impostare la registrazione di log di operazione di **Scanner** nel file. Per farlo, mettere il flag **Salvare report in file** e impostare i parametri richiesti di logging.

### Suoni (al richiamo delle configurazioni via il menu di gestione)

Nella sezione **Suoni** si può impostare la riproduzione di file audio per certi tipi di eventi. Per farlo, mettere il flag **Riprodurre suoni** e impostare i nome di file audio nei campi che corrispondono a eventi concreti.

## 7.6. Visualizzazione risultati di operazione e statistiche consuntivi per workstation

Con il menu di gestione della sezione **Rete antivirus** si possono visualizzare le seguenti informazioni:

- Tabelle - per visualizzare i dati di tabelle delle statistiche di operazione degli strumenti antivirus su workstation, dello stato di workstation o degli strumenti antivirus.
- Grafici - per visualizzare i grafici con le informazioni su infezioni, rilevati su workstation.

- Informazioni libere - per visualizzare e salvare i report, che contengono tutti i dati consuntivi statistici o riepiloghi personalizzati per i tipi di tabelle impostati.
- Quarantena - per visualizzazione e modifica remota dei contenuti di **Quarantena** su workstation.

## 7.6.1. Tabelle

***Per visualizzare le tabelle:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo.
2. Nel menu di gestione aperto (pannello a sinistra) scegliere la voce richiesta dalla sottosezione **Tabelle**.

Sezione del menu **Tabelle** contiene le voci seguenti:

- **Informazioni libere** - per visualizzare e salvare i report, che contengono tutti i dati consuntivi di statistiche o riepiloghi personalizzati per i tipi di tabelle impostati. Non viene visualizzata nel menu, se sono nascosti tutte le altre voci del menu nella sezione **Tabelle** (v. Dati consuntivi).
- **Infezioni** - per visualizzare le informazioni sul rilevamento dei virus (lista di oggetti contaggiati, virus, azioni di antivirus ecc).
- **Errori** - per visualizzare la lista di errori di scansione su workstation scelta per un certo periodo.
- **Statistiche** - per ottenere le statistiche sull'operazione degli strumenti antivirus su workstation (v. Statistiche).
- **Avvio/terminazione** - per visualizzare la lista dei componenti, avviati su workstation.
- **Virus** - per visualizzare le informazioni sul rilevamento di virus su workstation, raggruppate per i tipi di virus.
- **Stato** - per visualizzare le informazioni su stato insolito e (forse) richiedente intervento di workstation per un certo periodo (v. Stato).
- **Task** - per visualizzare la lista di processi, programmati per workstation per un certo periodo.

- **Statistiche complessive** - per ottenere le statistiche consuntive senza la suddivisione per le sessioni.
- **Basi virali** - per visualizzare le informazioni sui database dei virus installati: nome del file, che contiene il database dei virus concreto; versione del database; numero record nel database dei virus; data di creazione del database dei virus. La voce è disponibile solo alla scelta di workstation.
- **Moduli** - per visualizzare le informazioni dettagliate su tutti i plugin di **Dr.Web** Anti-virus: descrizione del plugin - il suo nome funzionale; file, che definisce il plugin singolo del prodotto; versione completa del plugin ecc. La voce è disponibile solo alla scelta di workstation.
- **Tutte le installazioni di rete** - per visualizzare la lista di installazioni del software su workstation.



Per visualizzare le voci nascoste della sezione **Tabelle** scegliere la voce **Amministrazione** del menu principale, nella finestra aperta scegliere la voce del menu di gestione **Configurazione Dr.Web Enterprise Server**. Nella scheda **Informazioni statistiche** mettere i flag corrispondenti (v. sotto), dopodiché premere su **Salva** e riavviare il **Server**.

**Tabella 7-4. Corrispondenza delle voci della sezione Tabelle e dei flag della sezione Dati statistici**

| Voci sezione Tabelle | Flag sezione Dati statistici |
|---|---|
| Infezioni | Infezioni del database |
| Errori | Errori scansione del database |
| Statistiche | Statistiche scansione del database |
| Avvio/terminazione | Informazioni su avvio/arresto dei componenti del database |
| Virus | Infezioni del database |
| Stato | Monitoraggio stato workstation |
| Task | Log esecuzione processi |
| Statistiche complessive | Statistiche scansione nel database |

| Voci sezione Tabelle | Flag sezione Dati statistici |
|---|---|
| Basi virali | Monitoraggio stato workstation<br>Monitoraggio database dei virus<br>Log esecuzione processi |
| Moduli | Lista plugin workstation nel database |
| Tutte le installazioni di rete | Informazioni sulle impostazioni di agent nel database |

La finestra di visualizzazione dei risultati di operazione di vari componenti e delle statistiche consuntive di workstation hanno la stessa interfaccia, e le azioni della specificazione delle informazioni, fornite da essi, sono le stesse.

Di seguito sono esaminati alcuni esempi di visualizzazione di statistiche consuntive via il **Centro gestione**.

## Statistiche

***Per ottenere le statistiche su operazione di strumenti antivirus su workstation:***

1. Scegliere nella lista la workstation richiesta o gruppo.

   Se è necessario visualizzare le statistiche per alcuni workstation o gruppi, è disponibile la scelta contemporanea di workstation richieste con i tasti SHIFT o CTRL.

2. Nel menu di gestione (pannello a sinistra) nella sezione **Tabelle** scegliere la voce **Statistiche**.
3. Si apre la finestra di statistiche. Di default vengono visualizzate le statistiche del giorno passato.
4. Per visualizzare i dati per un certo periodo indicare il periodo del tempo relativamente al giorno odierno nella lista a cascata o impostare un range qualsiasi nella barra degli strumenti. Per impostare un periodo qualsiasi inserire i dati richiesti o premere su icone del calendario accanto ai campi di dati. Per caricare i dati, premere sul tasto **Aggiorna**. Nella finestra saranno

caricate le tabelle con i dati statistici.

5. Nella sezione **Informazioni statistiche generali** sono riportati i dati consuntivi:
   - alla scelta di workstation - per le workstation scelte;
   - alla scelta di gruppi - per i gruppi scelti. Alla scelta di più gruppi saranno visualizzati solo i gruppi, che contengono le workstation;
   - alla scelta di workstation e di gruppi contemporaneamente - separatamente per tutte le workstation, comprese quelle che fanno parte dei gruppi non vuoti.
6. Per visualizzare le statistiche dettagliate di operazione di strumenti antivirus concreti, premere sul nome workstation nella tabella. Se sono stati scelti dei gruppi, premere sul nome del gruppo nella tabella delle statistiche generali, e quindi sul nome workstation nella tabella visualizzata. Si apre la finestra (o una sezione della finestra attuale), contenente la tabella con i dati statistici dettagliati.
7. Dalla tabella con le statistiche di operazione di strumenti antivirus di workstation o di gruppo si può aprire la finestra di configurazione di un componente antivirus concreto. Per farlo, premere sul nome corrispondente del componente nella tabella di statistiche.
8. Per ordinare i dati della colonna di tabella, premere sulla freccia corrispondente (ordine decrescente o crescente) nell'intestazione della colonna corrispondente.
9. Se è necessario salvare la tabella di statistiche per la stampa o per l'elaborazione successiva premere sul tasto  **Registra le informazioni in un file del formato CSV**, sul tasto  **Registra le informazioni in un file del formato HTML** o sul tasto  **Registra le informazioni in un file del formato XML**.
10. Per ottenere le statistiche consuntive non suddividendole per le sessioni, premere sul tasto **Statistiche complessive** nel menu di gestione. Si apre la finestra delle statistiche consuntive.

11. Per visualizzare le statistiche per gli eventi dei virus nel formato dei diagrammi, nel menu di gestione (pannello a sinistra) scegliere la voce **Grafici**. Si apre la finestra di visualizzazione dei diagrammi statistici (per la descrizione dettagliata v. sotto).

## Stato

***Per visualizzare le informazioni sullo stato di workstation per un certo periodo:***

1. Scegliere nel menu di gestione nella sezione **Tabelle** la voce **Stato**.
2. Le informazioni sullo stato di workstation sono visualizzati nella finestra automaticamente a seconda dei parametri, impostati nella barra degli strumenti.
3. Per limitare la lista dei messaggi dello stato solo ai messaggi di certa gravità, scegliere il livello di gravità nella lista a cascata **Serietà** nella barra degli strumenti. Di default è scelto il livello di gravità **Molto bassa**, il che corrisponde alla visualizzazione della lista massima.
4. Nella lista saranno incluse le workstation, che non hanno connessione al **Server** per un certo periodo di giorni. Indicare questo numero nel campo di input a sinistra della lista **Serietà**. Se si supera tale valore, la situazione è considerata critica, e tale informazione viene visualizzata nella finestra della sezione **Stato**.
5. Le azioni per specificazione e per formattazione di questa tabella sono analoghe alle descritte sopra per la tabella delle statistiche.



Si possono inoltre visualizzare i risultati di operazione e le statistiche di alcuni workstation. Per farlo, si deve marcare queste workstation nel catalogo della rete.

## 7.6.2. Grafici

### *Grafici di infezioni*

***Per visualizzare i grafici generali con le informazioni su infezioni rilevate:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo. Nel menu di gestione aperto (pannello a sinistra) scegliere nella sezione **Generali** la voce **Grafici**.
2. Si apre la finestra che contiene i seguenti dati grafici:
   - **Dieci virus più diffusi** - viene visualizzata la lista di dieci virus, che hanno infetto il numero maggiore dei file. Nel grafico si visualizzano i dati numerici per oggetti, che sono stati infetti da virus indicati.
   - **Attività dei virus giornaliera** - periodo di tempo impostato viene suddiviso per giorni. Nel grafico viene visualizzato il numero generale dei virus, rilevati nella durata di ogni giorno per tutti gli oggetti di rete scelti (workstation e gruppi). Il grafico viene visualizzato se il periodo di tempo impostato supera un giorno.
   - **Classi di infezioni** - si visualizzano i dati numerici per oggetti, suddivisi a secondo la classifica di infezioni.
   - **Quantità workstation infette in gruppo** - si visualizzano i dati numerici per numero di workstation infette per ogni gruppo, dove esse sono presenti.
   - **Azioni eseguite** - vengono visualizzati i dati numerici per oggetti infetti, a cui sono state applicate le azioni, previste dal software antivirus.
3. Per visualizzare i dati grafici per un periodo predefinito, scegliere un periodo dalla lista a cascata nella barra delle applicazioni: log per un certo giorno o per un mese. Si può scegliere qualsiasi periodo di date, per farlo inserire le date richieste o premere sui tasti di calendario accanto ai campi di date. Per visualizzare i dati premere sul tasto **Aggiorna**.

## *Grafici delle statistiche consuntive*

Dati grafici sono riportati nella voce **Grafici** della sezione **Generali** e in alcuni voci della sezione **Tabelle** del menu di gestione.

Nonostante l'oggetto scelto nella lista gerarchica (gruppo o workstation), vengono visualizzati diversi set di grafici. Nella tabella sottostante è riportata la lista dei grafici possibili e sezioni del menu di gestione, in cui tali grafici vengono visualizzati, nonostante l'oggetto scelto nella lista gerarchica.

**Tabella 7-5. Corrispondenza dei grafici alle voci scelte della lista gerarchica e alle sezioni del menu di gestione**

| Grafici | Per gruppi | Per workstation | Sezioni |
|---|---|---|---|
| Dieci virus più diffusi | + | + | Infezioni<br>Virus<br>Grafici |
| Dieci workstation più infette | + | | Infezioni |
| Tipi di infezioni | + | + | Virus |
| Risultati di installazioni | | | Tutte le installazioni di rete |
| Attività media dell'infezione | + | | Statistiche |
| Per numero errori | + | + | Errori |
| Per componenti | + | + | Errori |
| Risultati dei processi eseguiti | + | + | Processi |
| Classi di infezioni | + | + | Grafici |
| Azioni eseguite | + | + | Grafici |
| Attività dei virus giornaliera | + | + | Grafici |
| Quantità workstation infette in gruppo | + | | Grafici |

- **Dieci workstation più infette** - viene visualizzata la lista di dieci workstation, infette con numero maggiore di oggetti nocivi. Nel grafico vengono visualizzati i dati numerici per la quantità di oggetti nocivi, rilevati su queste workstation.
- **Tipi di infezioni** - grafico a torta, che visualizza il numero di oggetti nocivi rilevati per tipi di questi oggetti.
- **Risultati di installazioni** - grafico a torta, che visualizza il numero di tutte le installazioni, avviate da questo **Server**, suddivise per risultati di installazione. In caso di installazione fallita - con indicazione di errore. Il grafico viene visualizzato per tutte le installazioni da questo **Server**, nonostante l'oggetto, scelto nella lista gerarchica.
- **Attività media di infezione** - viene visualizzato il valore medio di infezione di workstation del gruppo scelto. Questo valore viene calcolato come somma di numero di tutti gli oggetti nocivi rilevati, divisa per numero oggetti scansionati su ogni workstation.
- **Per numero errori** - viene visualizzata la lista di workstation, su cui sono stati rilevati gli errori del funzionamento dei componenti antivirus singoli, installati su questi workstation. Nel grafico viene visualizzato il numero errori per workstation.
- **Per componenti** - viene visualizzata la lista dei componenti antivirus, installati su workstation, nel cui funzionamento ci sono stati degli errori. Nel grafico a torta viene visualizzato il numero errori generale di ogni componente.
- **Risultati di esecuzione dei processi** - viene visualizzata la lista dei processi, avviati su oggetti scelti. In grafico viene visualizzato il numero di avvii di ogni processo. Nella tabella sotto il grafico sono inoltre riportati i risultati di esecuzione dei compiti.

## 7.6.3. Informazioni libere

***Per visualizzare i dati consuntivi:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo. Nel menu di gestione aperto (pannello a sinistra) scegliere nella sezione **Tabelle** la voce **Informazioni libere**.
2. Si apre la finestra, che contiene i dati del report della tabella. Per poter includere nel report certi dati di statistiche, premere sul tasto Dati **consuntivi** nella barra degli strumenti e scegliere i tipi richiesti nella lista a cascata: **Statistiche**, **Infezioni**, **Task**, **Avvio/terminazione**, **Errori**. Statistiche, incluse in tali sezioni del report, corrispondono alle statistiche, contenute nelle voci corrispondenti della sezione **Tabelle**. Per visualizzare il report con tabelle scelte premere sul tasto **Aggiorna**.
3. Per visualizzare i dati per un certo periodo indicare un periodo di tempo in relazione alla data odierna nella lista a cascata o impostare un periodo di date nella barra degli strumenti. Per impostare un periodo inserire le date richieste o premere su icone del calendario accanto ai campi delle date. Per visualizzare i dati premere il tasto **Aggiorna**.
4. Se è necessario salvare il report per la stampa o per l'elaborazione successiva, premere sul tasto  **Registra le informazioni in un file del formato CSV**, sul tasto  **Registra le informazioni in un file del formato HTML** o sul tasto  **Registra le informazioni in un file del formato XML**.

## 7.6.4. Quarantena



Per poter gestire la **Quarantena** dal **Server** è necessario che le workstation con il plugin **Quarantena** installato operino nei SO, su cui si può installare **SpIDer Guard G3** (v. Requisiti di sistema).

Nel caso contrario la gestione remota non è disponibile. **Quarantena** non potrà neanche gestire i file della cartella `Infected.!!!`, e le informazioni su contenuti di **Quarantena** non verranno inviate al **Server**.

### *Contenuti di Quarantena*

I file possono essere aggiunti a **Quarantena**:

- da uno dei componenti antivirus, per esempio da **Scanner**,
- dall'utente manualmente tramite il gestore **Quarantena**.

Se spostati in **Quarantena**, i file vengono ricontrollati automaticamente. Durante tale scansione:

- viene determinato lo status dell'infezione, cioè la presenza e il tipo dell'infezione (poiché se il file è stato aggiunto a **Quarantena** manualmente, tali informazioni non sono disponibili),
- i nomi e i tipi delle infezioni vengono uniformati.

Inoltre, l'utente può ricontrollare file in **Quarantena** tramite il **Centro gestione** o tramite il gestore **Quarantena** sulla workstation.

### *Per visualizzare e modificare i contenuti di Quarantena nel Centro gestione:*

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome workstation o gruppo. Nel menu di gestione (pannello a sinistra) scegliere nella sezione **Generali** la voce **Quarantena**.
2. Si apre la finestra, che contiene i dati di tabella sullo stato

corrente di **Quarantena**.

Se è stata scelta una workstation, viene visualizzata la tabella con oggetti, che si trovano in **Quarantena** su questa workstation.

Se sono state scelte più workstation, un gruppo o più gruppi, viene visualizzato un set di tabelle, che contengono oggetti di quarantena per ogni singola workstation.

3. Per visualizzare i file, spostate in **Quarantena** in un certo periodo di tempo, indicare il periodo di tempo richiesto nella barra degli strumenti e premere sul tasto **Aggiorna**.
4. Per gestire i file che si trovano in **Quarantena**, mettere il flag sul file o sul gruppo dei file corrispondenti o su tutti i file di **Quarantena** (nella testata di tabella). Nella barra degli strumenti scegliere una delle seguenti azioni:

- **Ripristina i file** - per ripristinare i file da **Quarantena**.



Utilizzare tale funzionalità solo se si è convinti della sicurezza dell'oggetto.

Nel menu a cascata scegliere una delle varianti:

a) **Ripristina i file** - ripristinare il file al percorso originale sul computer (ripristinare il file nella cartella, dove si trovava prima di essere spostato in **Quarantena)**.

b) **Ripristina i file al percorso indicato** - spostare il file nella cartella, indicata dall'amministratore.

- **Rimuovi i file** - per eliminare i file scelti da **Quarantena** e dal sistema.
- **Scansiona i file** - per scansionare i file scelti in **Quarantena** di nuovo.
- **Esporta** - per copiare e salvare i file scelti in

**Quarantena**.

Dopo che file sospetti sono stati messi nella **Quarantena** locale sul computer dell'utente, è possibile copiare questi file tramite il **Centro gestione** e salvarli tramite il browser web ai fini, per esempio, del successivo invio al laboratorio di virus della società **Doctor Web**. Per salvare file, mettere flag di fronte ai file richiesti e premere sul tasto **Esporta**.

- Esportare i dati dello stato di **Quarantena** in file in uno dei seguenti formati:

 - scrivere i dati nel file nel formato CSV,

 - scrivere i dati nel file nel formato HTML,

 - scrivere i dati nel file nel formato XML.

# 7.7. Impostazioni di alcuni componenti antivirus



La composizione dei parametri di componenti e i consigli su uso di essi sono riportati nel manuale **Antivirus Dr.Web® per Windows. Manuale dell'utente**, nonché **Dr.Web® Agent per Windows. Manuale dell'utente**.

Di seguito sono riportate le impostazioni di alcuni componenti antivirus, che sono diversi dalle impostazioni, disponibili su workstation.

## 7.7.1. Configurazione di Controllo Ufficio per accedere alle risorse locali e di rete nel SO Windows®

Si può limitare accesso a certe risorse locali e alcuni nodi di Internet nel modo centralizzato. Per farlo, si utilizza il componente **Dr.Web Controllo Ufficio**.

***Configurazione del controllo Ufficio:***

1. Per aprire la finestra di modifica impostazioni scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica premere su nome di workstation o di gruppo. Nel menu di gestione aperto (pannello a sinistra) scegliere la voce **Dr.Web Controllo Ufficio**.
2. Nella scheda **Generali** scegliere le impostazioni del blocco e indicare le risorse (cartelle locali e file), a cui si deve proibire l'accesso:
   - Per attivare il blocco delle risorse locali e dei dispositivi rimovibili mettere il flag **Abitilare il blocco**.
   - Mettere il flag **Bloccare supporti rimovibili** per proibire l'accesso dell'utente ai dispositivi rimovibili.
   - Mettere il flag **Proteggere cartelle e file** per proibire l'accesso alle risorse indicate. I percorsi ai cartelli e ai file bloccati si impostano nel campo **Lista di cartelle e file protetti**. Per aggiungere un nuovo percorso premere sul tasto  , dopodiché modificare la riga aggiunta.



Se il file, al cui accesso si deve proibire, è indicato senza il percorso, si ritiene di essere locato nella cartella `%system32%` e nelle impostazioni di **Controllo Ufficio** del lato utente viene visualizzato con il prefisso `c:\windows\system32`.

3. Nella scheda **Accesso** mettere il flag **Filtraggio WWW** per poter configurare l'accesso ai domini di Internet. Mettere il flag **Bloccare tutti i siti** per proibire completamente l'accesso a Internet. Inserire nelle liste corrispondenti i domini, a cui si può

consentire/bloccare l'accesso. Per creare un record nuovo premere il tasto  e inserire i valori nella finestra aperta.

Nella sezione **Bloccare i contenuti** mettere i flag vicino a categorie dei siti da bloccare. Questi flag attivano il filtro incorporato e bloccano i siti web che corrispondono a tali categorie.

4. Finita la configurazione, premere sul tasto **Salva**. Le configurazioni entrano in vigore dopo la conferma di nuova configurazione workstation.



Nelle configurazioni del Controllo Ufficio è proibito proteggere le seguenti cartelle, comprese le loro cartelle radici:

- `%SYSTEMROOT%`,
- `%USERPROFILE%`,
- `%PROGRAMFILES%`.

Si possono bloccare le loro sottocartelle.

**Controllo Ufficio** non permette di bloccare i file e le cartelle di rete.

Se per una workstation è consentito modificare la configurazione di **Controllo Ufficio** (v. Configurazione diritti utenti), l'utente ha la possibilità di limitare l'accesso alle risorse per conto proprio. In questo caso rimane la possibilità di impostare le configurazioni sul **Server**. Le impostazioni, configurate sul **Server**, verranno automaticamente aggiornate dal lato utente.



Nel caso di errore di amministrazione nella configurazione del **Controllo Ufficio** sul **Server** (errore nel percorso alle risorse bloccate o impostazione della cartella, il cui blocco è proibito), le impostazioni vengono aggiornate nel lato utente, ma il blocco non diventa attivo. In questo caso non si communica di errore amministrazione.

### 7.7.2. Configurazione del componente MailD per protezione di indirizzi di posta nei SO UNIX® e Mac OS X

Nel funzionamento di **Agent** nei SO della famiglia UNIX e Mac OS X si può impostare la lista di indirizzi di posta protetti. Si possono impostare 15, 30, 50 o più indirizzi di posta che verranno controllati dal componente **Dr.Web MailD**.



Si può visualizzare il numero di indirizzi di posta protetti nel file della chiave di **Agent** (`agent.key`).

***Per impostare la lista di indirizzi e-mail protetti:***

1. Scegliere nella lista gerarchica del **Centro gestione** una workstation o un gruppo di workstation e nel menu di gestione (pannello a sinistra) cliccare sulla voce **Indirizzi email**.
2. Nella finestra aperta inserire nel campo l'indirizzo e-mail richiesto.
3. Per aggiungere un indirizzo nuovo premere il tasto  . Ogni nuovo indirizzo deve essere inserito in una riga nuova.
4. Per eliminare un indirizzo premere su tasto  accanto al campo corrispondente.
5. Per salvare le modifiche apportate premere su **Salva.**

## 7.8. Invio messaggi all'utente

L'amministratore di sistema può inviare agli utenti i messaggi informativi di qualsiasi contenuto, che includono:

- testo di messaggio;
- link alle risorse Internet;
- logo della società (o qualsiasi immagine grafico);

- nella testata della finestra inoltre viene indicata la data precisa di ricezione del messaggio.

Tali messaggi sono visualizzati dal lato utente come le finestre pop-up (v. immagine 7-1).

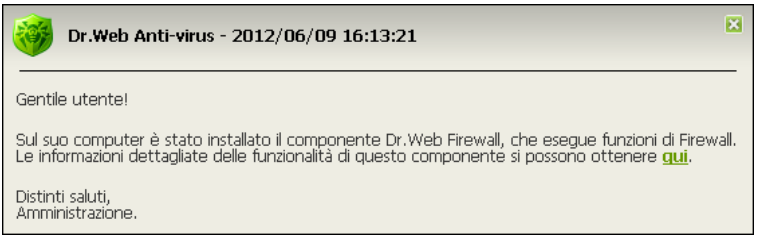

Dr.Web Anti-virus - 2012/06/09 16:13:21
Gentile utente!
Sul suo computer è stato installato il componente Dr.Web Firewall, che esegue funzioni di Firewall. Le informazioni dettagliate delle funzionalità di questo componente si possono ottenere qui.
Distinti saluti,
Amministrazione.

**Immagine 7-1. Finestra di messaggio lato utente**

### *Per inviare un messaggio all'utente:*

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**.
2. Nella finestra aperta nella lista gerarchica scegliere workstation o gruppo e premere su **Generali** → **Inviare messaggi alle postazioni** nella barra degli strumenti.

Nella finestra aperta riempire i seguenti campi:

- **Testo di messaggio** - campo obbligatorio. Contiene il messaggio stesso.
- **Visualizzare il logo della società nel messaggio** - attivare tale flag per visualizzare un oggetto graifco nella testata della finestra del messaggio. Per caricare il file di logo dalla risorsa locale si deve premere sul tasto **Sfogliare** a destra del campo **File con logo** e scegliere l'oggetto necessario nel browser aperto per file system.

  Si può impostare la testata del messaggio o il nome della società nel campo **Nome**. Tale testo sarà visualizzato nella testata della finestra del messaggio (a destra del logo). Se questo campo rimane vuoto, se sul suo posto nella finestra del messaggio sarà visualizzato il testo, contenente informazioni su **Agent**.

Nel campo **URL** si deve indicare il link sulla pagina web, che sarà aperta quando si preme sul logo (anche quando si preme sulla testata di finestra, se è stato indicato nel campo **Nome**).

Se il logo non è impostato, o la dimensione del logo supera la dimensione massima ammissibile (v. Formato del file di logo, p. 3), al suo posto nella finestra del messaggio si visualizza l'icona di **Enterprise Agent**.

Con il flag attivato **Visualizzare il logo della società nel messaggio** diventa attivo il flag **Utilizzare trasparenza**. Mettere tale flag per utilizzare la trasparenza nell'immagine del logo (v. Formato del file di logo, p. 4).

- **Visualizzare il link nel messaggio** - attivare tale flag per includere i link alle risorse web nel messaggio all'utente. Per aggiungere il link si deve:
  1. Nel campo **URL** inserire il link alla risorsa Internet.
  2. Nel campo **Testo** indicare il nome del link - il testo, che viene visualizzato al posto del link nel messaggio.
  3. Nel campo **Testo messaggio** indicare tag `{link}` dappertutto dove si deve aggiungere il link. Nel messaggio finale al suo posto viene inserito il link con i parametri indicati. Numero dei tag `{link}` nel testo non è limitato, ma tutti i loro parametri saranno uguali (dei campi **URL** e **Testo** rispettivamente).

**Per esempio**:

Per avviare il messaggio, riportato nell'immagine 7-1, sono stati impostati i seguenti parametri di link:

**Testo del messaggio**:

```
Gentile utente!


Sul suo computer è stato installato il
componente Dr.Web Firewall, che esegue
funzioni di Firewall.
Le informazioni dettagliate delle
```

```
funzionalità di questo componente si possono
ottenere {link}.


Distinti saluti,
Amministrazione.
```

**URL**: `http://drweb.com/`

**Testo**: `qui`

- **Visualizzare il risultato di consegna** - mettere questo flag per ricevere report sulla spedizione del messaggio all'utente.

## *Formato del file di logo*

File con immagine grafica (logo), incluso nel messaggio, deve soddisfare le seguenti condizioni:

1. Formato grafico del file - bmp.
2. Profondità di colore (bit depth) - qualsiasi (8 - 24 bit).
3. Dimensione massima della parte visibile del logo è pari al 120x90 px (larghezza x altezza). In più 2x2 px - è la margine per la cornice dei pixel trasparenti (v. p. 4), cioè dimensione massima dell'immagine è di 122x92 px (v. figura 7-2).

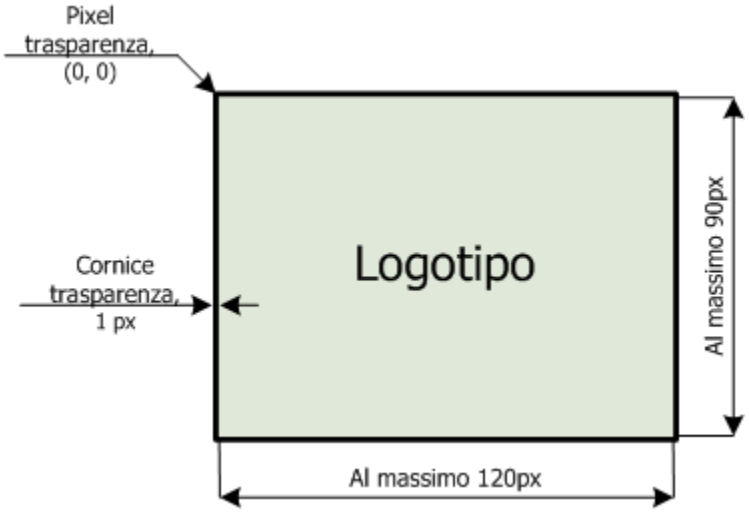



**Immagine 7-2. Formato del file di logo**

4. Nel caso se all'invio del messaggio è stata attivata l'opzione **Utilizzare trasparenza**, il primo pixel nella posizione (0,0) viene dichiarato *trasparente*. Tutti i pixel, che hanno lo stesso colore, diventano trasparenti, cioè al loro posto si visualizza lo sfondo della finestra del messaggio.

   Se si attiva l'opzione **Utilizzare trasparenza** per il logo rettangolare, si consiglia di fare una cornice rettangolare per evitare l'impostazione scorretta di pixel del logo stesso come "trasparenti".

   Impostazione di opzione **Utilizzare trasparenza** è utile nel caso della forma non standard (non rettangolare) del logo per escludere lo sfondo indesiderabile che completa la parte informativa per renderla rettangolare. Per esempio, se si utilizza come il logo l'immagine, riportato nell'immagine 7-3, lo sfondo viola viene escluso (diventa trasparente).



**Immagine 7-3. Logo della forma non standard**

Prima di inviare il messaggio all'utente (soprattutto a più indirizzi), si consiglia di inviarlo preliminarmente a qualsiasi computer con **Agent** installato per controllare la correttezza del risultato.

# Capitolo 8. Configurazione di Dr.Web Enterprise Server

## 8.1. Configurazione di Dr.Web Enterprise Server

***Per impostare i parametri di configurazione di Dr.Web Enterprise Server:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**.
2. Nella finestra aperta scegliere la voce del menu di gestione **Configurazione Dr.Web Enterprise Server**.
3. Si apre la finestra delle impostazioni del **Server**.



I valori dei campi, marcati con *, sono obbligatori da definire.

### Scheda Generali

Parametro **Nome** definisce il nome di questo **Server**. Se non è impostato, si applica il nome del computer, sul quale funziona il software di **Enterprise Server**.

Parametro **Filoni** definisce il numero dei flussi per elaborazione dei dati, che arrivano da **Agent**. Si consiglia di modificare il valore predefinito solamente dopo l'approvazione del supporto tecnico.

Parametro **Connessioni alla base database di dati** definisce il numero delle connessioni di **Server** al database. Si consiglia di modificare il valore predefinito solamente dopo l'approvazione del supporto tecnico.

Nel campo **Coda di autorizzazione** si imposta il numero massimo di workstation in attesa ad essere autorizzati sul **Server**. Si può indicare qualsiasi numero intero.

Nella lista a cascata **Traffico di aggiornamenti** si imposta la banda massima di passaggio di traffico di rete durante la trasmissione di aggiornamenti tra **Server** e **Agent**. A questo:

- Se tale parametro ha il valore **Illimitata**, aggiornamenti vengono passati a vari **Agent** senza limitazione della larghezza di banda del traffico di rete.
- Se per questo parametro è impostato un altro valore, diverso da **Illimitata** (valore numerico concreto), aggiornamenti vengono passati nei limiti della banda impostata del passaggio del traffico di rete totale di aggiornamenti di tutti gli **Agent**.

Nella lista a cascata **Nuovi arrivi** si imposta la politica di connessione delle workstation nuove (v. Politica connessione workstation).

I flag **Trasferisci le postazioni non autorizzate in nuovi arrivi** prescrive al programma di ripristinare i parametri di connessione al **Server** delle workstation, che non hanno passato l'autorizzazione. Questa opzione potrebbe essere utile alla modifica delle impostazioni di **Server** (come la chiave aperta) o al cambio di database. In tali casi le workstation non riescono a connettersi e si richiede di ottenere di nuovo i parametri nuovi per accedere al **Server**.

Nelle lista a cascata **Crittografia** e **Compressione** si sceglie la politica di codifica e di compressione del traffico tra **Enterprise Server**, **Agent** e **Centro gestione** (per più informazioni su questi parametri v. Utilizzo codifica e compressione del traffico).

Si può inoltre modificare lo stato dei seguenti flag:

- **Mostra i nomi di dominio** prescrive al programma di scrivere nel file del log non indirizzi IP delle workstation, ma i loro nomi di domini.
- **Sostituisci i nomi NetBIOS** prescrive di visualizzare nella cartella della rete antivirus del **Centro gestione** non i nomi delle workstation, ma i loro nomi di domini (se non è possibile definire il nome di dominio si visualizzano gli indirizzi IP).



Tutti e due flag **Mostra i nomi di dominio** e **Sostituisci i nomi NetBIOS** di default sono tolti. Con la configurazione del servizio DNS scorretta l'attivazione di queste possibilità potrebbe rallentare notevolmente il funzionamento del **Server**. Se si attiva una di queste modalità si consiglia di consentire il caching dei nomi su server DNS.



Se il flag **Sostituisci i nomi NetBIOS** è installato, e nella rete antivirus si utilizza il **Server proxy**, per tutte le workstation, connesse al **Server** via il **Proxy server**, nel **Centro gestione** come nomi di workstation viene visualizzato il nome del computer, su cui è installato il **Proxy server**.

- **Sincronizza le descrizioni delle postazioni** - prescrive la sincronizzazione della descrizione del computer dell'utente con la descrizione di workstation nel **Centro gestione**. Se nel **Centro gestione** non c'è la descrizione di workstation, in questo campo verrà inserita la descrizione del computer del lato utente. Se le descrizioni sono diverse, i dati del **Centro gestione** saranno sostituiti con i dati dell'utente.

## Scheda Dati Statistici

Nella scheda **Informazioni statistiche** vengono impostate le informazioni di statistiche, che vengono registrati nel report e salvati nel database del **Server**.

***Per aggiungere al database il tipo di informazione corrispondente mettere i seguenti flag:***

- **Quarantena** - permette di scrivere lo stato di **Quarantena** su workstation.
- **Lista di moduli delle postazioni nella base di dati** - permette di scrivere i contenuti dei plugin di **Antivirus** su workstation.
- **Lista dei componenti installati nella base di dati** - permette di scrivere, quali componenti di **Antivirus** (**Scanner**, **Monitoraggio** ecc.) sono installati su workstation.

- **Informazioni su avvio/terminazione di componenti nella base di dati** - permette di scrivere le informazioni su avvio e arresto del funzionamento dei componenti di **Antivirus (Scanner**, **Monitoraggio** ecc.) su workstation.
- **Infezioni nella base di dati** - permette di scrivere i dati statistici delle infezioni, rilevate su workstation.
- **Errori di scansione nella base di dati** - permette di scrivere le informazioni su tutti gli errori della scansione su workstation.
- **Statistiche di scansione nella base di dati** - permette di scrivere i risultati della scansione su workstation.
- **Informazioni su installazioni dell'agent nelle base di dati** - permette di scrivere le informazioni sulle installazioni di **Agent** su workstation.
- **Log di esecuzione del task** - permette di scrivere nel database i risultati di esecuzione dei processi su workstation.
- **Monitoraggio dello stato delle postazioni** - permette di registrare le variazioni dello stato di workstation e scrivere le informazioni nel database.
- **Monitoraggio delle basi di dati di virus** - permette di gestire lo stato (contenuti, modifiche) dei database dei virus su workstation e scrivere le informazioni nel database.

***Per visualizzare le informazioni statistiche:***

1. Scegliere la voce del menu principale **Rete antivirus**.
2. Nella lista gerarchica scegliere workstation o gruppo.
3. Aprire sezione corrispondente del menu di gestione (v. tabella sotto).



Descrizione dettagliata di dati statistici è riportata nella sezione Visualizzazione di risultati del funzionamento e di statistiche totali per workstation.

Nella tabella sottostante è riportata la corrispondenza dei flag della sezione **Informazioni statistiche** nelle impostazioni di **Server** e di voci del menu di gestione sulla pagina **Rete antivirus**.

Se si tolgono i flag nella scheda **Informazioni statistiche**, le voci corrispondenti saranno nascoste dal menu di gestione.

**Tabella 8-1. Corrispondenza delle impostazioni del Server e delle voci del menu di gestione**

| Impostazioni del server | Voci del menu |
|---|---|
| Quarantena | Generali → Quarantena |
| Lista di moduli delle postazioni nella base di dati | Tabelle → Plugin |
| Lista dei componenti installati nella base di dati | Generali → Componenti installati |
| Informazioni su avvio/terminazione di componenti nella base di dati | Tabelle → Avvio/Arresto |
| Infezioni nella base di dati | Tabelle → Infezioni<br>Tabelle → Virus |
| Errori di scansione nella base di dati | Tabelle → Errori |
| Statistiche di scansione nella base di dati | Tabelle → Statistiche<br>Tabelle → Statistiche totali |
| Informazioni su installazioni dell'agent nelle base di dati | Tabelle → Tutte le installazioni di rete |
| Log di esecuzione del task | Tabelle → Processi<br>Tabelle → Database dei virus |
| Monitoraggio dello stato delle postazioni | Tabelle → Stato<br>Tabelle → Database dei virus |
| Monitoraggio delle basi di dati di virus | Tabelle → Database dei virus |

## Scheda Statistiche

Nella scheda **Statistiche** si impostano i parametri di invio statistiche di eventi virus alla società **Doctor Web**.

Per attivare l'invio delle statistiche mettere il flag su **Statistiche**. Saranno disponibili i seguenti campi:

- **Intervallo** - intervallo di invio delle statistiche in minuti;
- **Indirizzo del server** - indirizzo IP o nome DNS e porta del server di statistiche (predefinito `stat.drweb.com:80`);
- **URL** - cartella su server di statistiche (predefinito `/update`);
- **Identificatore del client** - chiave MD5 del **Server** (si trova nel file della chiave del **Server** `enterprise.key`);
- **Utente** - nome utente per registrare le statistiche. Il nome utente si può ricevere dal **Supporto tecnico** della società **Doctor Web**;
- **Password** - password per registrare le statistiche. La password si può ricevere dal **Supporto tecnico** della società **Doctor Web**;
- **Server proxy** - se necessario, si può indicare l'indirizzo del server proxy per inviare le statistiche;
- **Utente dell proxy** - nome utente del server proxy (non si indica all'autorizzazione anonima del proxy);
- **Password del'utente del proxy** - password per accedere al server proxy (non si indica all'autorizzazione anonima del proxy).

I campi obbligatori sono solamente **Indirizzo del server** di statistiche e **Intervallo** di invio di statistiche.

Per salvare le modifiche apportate premere il tasto **Salva**.

## Scheda Sicurezza

Nella scheda **Sicurezza** si impostano le limitazioni di indirizzi di rete, da quali **Agent**, installazione di rete ed altri ("vicini") **Server** possono accedere a tale **Server**.

La gestione del report di audit del **Server** è eseguita con i seguenti flag:

- **Verifica delle operazioni** consente di gestire il report di audit delle operazioni dell'amministratore con **Centro gestione**, nonché la registrazione del report nel database.
- **Verifica delle operazioni interne del server** consente di gestire il report di audit di operazioni interne del **Server** e la registrazione del report nel database.



Si può visualizzare audit report, scegliendo nel menu principale **Amministrazione** la voce **Log di verifica report**.

Nella scheda **Sicurezza** ci sono schede supplementari **Agent**, **Installazione** e **Adiacenti**, dove si impostano le limitazioni per i tipi di connessioni corrispondenti.

***Per impostare la limitazione di accesso per qualche tipo di connessione:***

1. Passare alla scheda corrispondente (**Agent**, **Installazione** o **Adiacenti**).
2. Per consentire tutte le connessioni, togliere il flag da **Usa questa lista dell'accesso**.
3. Per impostare le liste di indirizzi consentiti o bloccati, mettere il flag su **Usa questa lista dell'accesso**.
4. Per consentire l'accesso da un certo indirizzo TCP, includerlo nella lista **TCP: permesso** o **TCPv6: permesso**.
5. Per bloccare qualche indirizzo TCP, includerlo nella lista **TCP: prohibito** o **TCPv6: prohibito**.

***Per modificare la lista di indirizzi:***

1. Inserire l'indirizzo di rete nel campo corrispondente e premere il tasto **Salva**.
2. Per aggiungere il nuovo campo di indirizzo, premere il tasto  della sezione corrispondente.

3. Per eliminare il campo premere il tasto  .

   Indirizzo di rete viene definito come: *<indirizzo-IP>*/[*<prefisso>*].



Le liste per inserire gli indirizzi TCPv6 saranno visualizzati solo se sul computer è installata l'interfaccia IPv6.

**Esempio di utilizzo del prefisso:**

1. Prefisso 24 significa le reti con la maschera: `255.255.255.0`

   Contiene 254 indirizzi

   Indirizzi host in queste reti sono del tipo: `195.136.12.*`

2. Prefisso 8 significa le reti con la maschera `255.0.0.0`

   Contiene fino a 16387064 indirizzi (256*256*256)

   Indirizzi host in queste reti sono del tipo: `125.*.*.*`

Nello stesso modo si impostano le limitazioni per indirizzi IPX.

Indirizzi, non inclusi in nessuna lista, sono consentiti o bloccati secondo se è messo il flag **Priorità del divieto**: se il flag è messo, gli indirizzi, non inclusi in nessuna lista (o inclusi in tutte e due), sono bloccati. Nel caso contrario, tali indirizzi sono consentiti.

## Scheda Base di dati

Nella scheda **Base di dati** si imposta la scelta del DBMS per conservare il log centralizzato della rete antivirus e le sue impostazioni (per più informazioni su questi parametri v. Configurazione di modalità di operazione con database).

## Scheda Avvisi

I parametri nella scheda **Avvisi** permettono di configurare la modalità di avvisi di amministratori della rete antivirus e di altre persone di attacchi dei virus e di altri eventi, rilevati da componenti di **Dr.Web Enterprise Security Suite** (per più informazioni su questa impostazione v. Configurazione avvisi).

## Scheda Trasporto

Sulla scheda **Trasporto** si impostano i parametri di protocolli di trasporto, utilizzati dal **Server**.

Per ogni protocollo nel campo **Nome** si può indicare il nome di **Enterprise Server**. Se non è indicato, si utilizza il nome, impostato nella scheda **Generali** (v. sopra, in particolare, se nella scheda indicata non è impostato nessun nome, si utilizza il nome del computer). Se per protocollo è impostato un nome diverso dal definito nella scheda **Generali**, viene utilizzato il nome dalla descrizione del protocollo. Questo nome è utilizzato dal servizio di rilevamento di **Server** da **Agent** ecc.

Nel campo **Indirizzo** si deve indicare l'indirizzo di interfaccia, ascoltata da **Server** per comunicare con **Agent**, installati sulle workstation.

Nel campo **Indirizzo del cluster** si deve obbligatoriamente indicare l'indirizzo dell'interfaccia, ascoltata da **Server** per comunicazione con **Agent** e **Installazione di rete** alla ricerca dei **Enterprise Server** attivi della rete. Per descrizione più approfondita v. sezione Servizio rilevamento Server.

Questi parametri vengono impostati nel formato di indirizzo di rete, riportato in Allegato E. Specifica di indirizzo di rete.

## Scheda Moduli

Nella scheda **Moduli** si imposta la modalità di utilizzo dei protocolli di comunicazione di **Server** con altri componenti di **Dr.Web ESS**.

Di default è consentita la comunicazione con:

- **Enterprise Agent**,
- componente **NAP Validator**,
- **Programmi di installazione di rete di Agent**.

Comunicazione di **Enterprise Server** con altri **Enterprise Server** di default è disattivata. Configurando la rete a più server (v. Particolarità di rete con più server) attivare questo protocollo, mettendo il flag corrispondente.

## Scheda Posizione

Sulla scheda **Posizione** si può indicare l'informazione supplementare del computer, dove è installato il software di **Enterprise Server**.

## 8.1.1. Utilizzo di codifica e compressione traffico

Rete antivirus di **Dr.Web Enterprise Security Suite** permette di codificare il traffico tra **Server** e workstation **(Enterprise Agent**), tra **Enterprise Server** (con la configurazione di rete a più server), e inoltre tra **Server** e **Installazione di rete**. Questa modalità viene utilizzata per evitare un'eventuale divulgazione delle chiavi di utenti, nonché delle informazioni di utenze e di utenti di rete antivirus.

Rete antivirus di **Dr.Web Enterprise Security Suite** utilizza i mezzi di firma digitale e di codifica crittograficamente sicuri, basati sul concetto di coppie delle chiavi aperte e chiuse.

Politica di utilizzo di codifica è impostata separatamente per ogni componente della rete antivirus, le impostazioni di altri componenti devono corrispondere alle impostazioni del **Server**.

***Per impostare le politiche di codifica e di compressione per Dr.Web Enterprise Server:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**.

2. Nella finestra aperta scegliere la voce del menu di gestione **Configurazione di Dr.Web Enterprise Server**.
3. Nella scheda **Generale** scegliere nelle liste a cascata **Crittografia** e **Compressione** una delle seguenti varianti:
   - **Sì** — codifica (o compressione) del traffico con tutti i componenti è obbligatoria (predefinito per la codifica, se durante l'installazione del **Server** non è stato impostato altrimenti),
   - **Possibile** — codifica (o compressione) vengono eseguiti per il traffico con i componenti, le cui impostazioni non lo bloccano,
   - **No** — codifica (o compressione) non si supportano (predefinito per la compressione, se durante l'installazione del **Server** non è stato impostato altrimenti).

Durante il coordinamento delle impostazioni di politica di codifica sul **Server** o su altro componente (**Agent** o **Installazione di rete**) si deve considerare che una serie di combinazioni delle impostazioni non è ammissibile e la loro scelta comporta la perdita di connessione tra **Server** e componente.

Nella tabella 8-2 sono raccolti i dati, con le quali impostazioni la connessione tra **Server** e componente è codificato (+), con quali – non codificato (–), e quali combinazioni non sono ammissibili (**Errore**).

**Tabella 8-2. Compatibilità delle impostazioni di politica di codifica**

| Impostazioni Server / Impostazioni componente | Sì | Possibile | No |
|---|---|---|---|
| Sì | + | + | Errore |
| Possibile | + | + | – |
| No | Errore | – | – |



Utilizzo di codifica del traffico crea un carico notevole di elaborazione dei dati sui computer con le prestazioni minime ammissibili per i componenti installati. Se la codifica del

traffico non è richiesta per fornire la sicurezza supplementare, si può non utilizzare questa modalità. Inoltre la codifica del traffico non è consigliabile per reti grandi (più di 2000 client). In questo caso si deve conseguentemente passare il **Server** e i componenti prima nella modalità **Possibile**, non ammettendo la creazione di coppie incompatibili di **Installazione di rete-Server** e **Agent-Server**. Non rispetto di questa regola potrebbe portare alla mancata gestione del componente e alla necessità di reinstallarlo.



Di default **Enterprise Agent** viene installato con le impostazioni di codifica **Possibile**. Questa combinazione significa che la codifica di default viene eseguita, ma può essere cancellata con la modifica delle impostazioni di **Enterprise Server**.

Visto che il traffico tra i componenti (soprattutto **Server**) può essere abbastanza significativo, la rete antivirus permette di impostare la compressione di tale traffico. La configurazione di politica di compressione e la compatibilità di queste impostazioni su vari componenti sono completamente uguali a quelle descritte sopra per la codifica, con la differenza che per il **Server** la configurazione di compressione di default è **No**.



Utilizzo di compressione diminuisce il traffico, ma aumenta notevolmente il carico di elaborazione di dati sui computer, più di codifica.

## 8.1.2. Configurazione modalità operazione con database



Si può ottenere la struttura del database di **Enterprise Server** sulla base dello script sql `init.sql`, locato nella sottocartella `etc` della cartella di installazione di **Enterprise Server**.

***Per configurare i parametri di operazione con il database:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**.
2. Nella finestra aperta scegliere la voce del menu di gestione **Configurazione di Dr.Web Enterprise Server**.
3. Passare alla scheda **Basa di dati** e scegliere nella lista a cascata **Basa di dati** il tipo del database:
   - **IntDB** – database incorporato (componente di **Enterprise Server**),
   - **MS SQL CE** – database esterno per **Server**, che operano con il SO Windows,



Database esterno **MS SQL CE** ha la produttività bassa ed è pegiore per questo indicatore del database interno.

Con il carico superiore a 30 workstation client non si consiglia di utilizzare questo database.

Comunque il database **MS SQL CE** può essere utilizzato per creare i report via API ADO.NET. Se questa possibilità non è richiesta, si consiglia di utilizzare il database interno o uno di altri eventuali database esterni.

   - **ODBC** (per i **Server**, che operano con il SO Windows) o **PostgreSQL** (per i **Server** con il SO della famiglia UNIX) – database esterno,
   - **Oracle** – database esterno (per le piattaforme oltre FreeBSD).



Se si utilizza il **DBMS Oracle** esterno, si deve installare l'ultima versione del **driver ODBC**, fornita con questo DMBS. Utilizzo del **driver ODBC** Oracle, fornito da **Microsoft**, è categoricamente sconsigliato.

Per il database incorporato, se è necessario, inserire nel campo **File** il percorso completo al file con il database e impostare la dimensione della memoria cash e la modalità di registrazione dei dati.

Le opzioni per i database esterni sono descritte in dettagli in allegati (v. Allegato B. Impostazioni, necessarie per l'utilizzo di DMBS. Opzioni driver DBMS).

Di default è previsto l'utilizzo del DBMS incorporato. La scelta di questa modalità crea il carico di elaborazione dei dati notevole sul Server. Con la dimensione significativa della rete antivirus si consiglia di utilizzare il DBMS esterno.



Utilizzo del database interno è ammissibile alla connessione al **Server** di meno di 200-300 workstation. Se lo permette la configurazione hardware del computer, su cui è installato **Enterprise Server**, e il carico di altri processi, eseguiti su questo computer – si possono connettere fino a 1000 workstation.

Altrimenti si deve utilizzare il database interno.

Con utilizzo di database interno e con connessione al **Server** di più di 10000 workstation si consiglia di eseguire i seguenti requisiti minimi:

- processore con frequenza 3GHz,
- memoria operativa - superiore a 4 GB per **Enterprise Server**, superiore a 8 GB – per il database server,
- il SO della famiglia UNIX.



È prevista la possibilità di eseguire le operazioni, legate alla pulizia del database, utilizzata da **Enterprise Server**, cioé: eliminazione di record di eventi, nonché le informazioni su workstation, che non hanno frequentato il **Server** per un certo periodo. Per pulire il database passare alla sezione orario Server e creare il processo corrispondente.

## 8.1.3. Configurazione avvisi

***Per configurare modalità invio avvisi di eventi nella rete antivirus:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**.
2. Nella finestra aperta scegliere la voce del menu di gestione **Configurazione Dr.Web Enterprise Server**.
3. Passare alla scheda **Avvisi** e scegliere la modalità richiesta di avvisi nella lista a cascata **Avvisi**:
   - **Non abilitare** – non avviare avvisi (modalità predefinita),
   - **Posta elettronica** – inviare avvisi per posta elettronica,
   - **Messaggi atraverso la rete di Windows** – inviare avvisi, utilizzando **Windows Messenger** (solo per **Server** con il SO Windows).

### *Avvisi per posta elettronica*

Per avvisi via posta elettronica impostare i seguenti parametri:

- **Mittente** – indirizzi di mittente di avviso.
- **Destinatario** – indirizzo di un destinatario o di più destinatari del messaggio. Per aggiungere un altro campo del destinatario premere sul tasto  .
- **Server SMTP**, **Porta** – indirizzo e porta del server SMTP, a cui si deve inviare la posta elettronica.
- **Utente**, **Password** (**Password ripetuta**) – se necessario, impostare nome utente e password per autorizzazione sul server SMTP.

Se necessario, mettere i seguenti flag:

- **Modalità debug** – per ottenere il log dettagliato della sessione SMTP.
- **Utilizza TLS/SSL per criptare il traffico** – per utilizzare la

codifica *TLS/SSL* del traffico durante l'invio di avvisi per posta elettronica.

- **Permetti l'autorizzazione plain text** – per utilizzare autenticazione testo in chiaro sul server di posta.
- **Permetti l'autorizzazione CRAM-MD5** – per utilizzare autenticazione *CRAM-MD5* sul server di posta.

Nella sezione **Messaggi consentiti** mettere i flag solo su eventi, di cui avvisi verranno inviati per posta elettronica.

## Messaggi in rete Windows



Sistema messaggi in rete Windows opera solamente nel SO Windows con supporto del servizio Windows Messenger (Net Send).

Il SO Windows Vista e superiori non supportano il servizio Windows Messenger.

Per messaggi in rete del SO Windows impostare la lista dei nomi di computer di destinatari dei messaggi.

Per aggiungere un nuovo campo premere sul tasto  e inserire il nome del computer nel campo apparso. Per eliminare un campo premere sul tasto  .

Nella sezione **Avvisi consentiti** mettere i flag su eventi, di cui si invieranno degli avvisi.

## Template avvisi

Il testo di avviso è definito dal template di avviso. I template di avvisi stanno nella sottocartella `var/templates` della cartella di installazione del **Server**. Per configurare il testo di avviso, inviato a un certo evento, modificare il template corrispondente.

Durante la preparazione di avviso il sistema di avvisi sostituisce le variabili di template (nelle parentesi graffe) con il testo concreto, che dipende dalle sue configurazioni attuali. La lista delle variabili disponibili è riportata negli allegati (v. Allegato D. Parametri template sistema avvisi).

Per modificare i template si consiglia di utilizzare **Editor dei template.** Per farlo:

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Editor dei template**.
2. Si apre la finestra di editor di template. Per modificare un template, sceglierlo nella lista.
   - nel campo **Oggetto** si può modificare oggetto del messaggio inviato.
   - nel campo **Intestazioni** si impostano, se necessario, le intestazioni supplementari del messaggio elettronico.
   - nel campo **Messaggio** si imposta il template del testo di avviso.

   Per aggiungere variabili si possono utilizzare le liste a cascata nell'intestazione del messaggio.
3. Per salvare il template modificato premere sul tasto **Salva**.



Se per modificare i template si utilizza un editor esterno, salvare i file di template nella codifica **UTF-8**. Si sconsiglia fortemente di utilizzare il **Blocco note** ed altri editor, che inseriscono nel testo il marcatore dell'ordine dei byte (BOM) per definire codifica **UTF-8**, **UTF-16** o **UTF-32**.

# 8.2. Gestione del log di server

**Enterprise** registra il log di eventi, relativi al suo funzionamento. Il nome del file di log – `drwcsd.log`.

Percorso predefinito al file di log:

- Nei SO **UNIX**:
  - in Linux: `/var/opt/drwcs/log/drwcsd.log`;
  - in FreeBSD e Solaris: `/var/drwcs/log/drwcsd.log`.
- Nei SO **Windows**: nella sottocartella `var` della cartella di installazione del **Server**.

Il file ha il formato semplice di testo (v. Allegato L. Formato dei file di log).



Il log del **Server** viene utilizzato per il debugging, nonché per risolvere i guasti nel caso del funzionamento non ordinario dei componenti della rete antivirus.

## 8.3. Configurazione orario di Dr.Web Enterprise Server

***Per configurare orario di esecuzione di processi per Dr.Web Enterprise Server:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Orario Dr.Web Enterprise Server**. Si apre la lista attuale di processi del **Server**.
2. Per eliminare un compito dalla lista, metterne accanto il flag, dopodiché scegliere nella barra degli strumenti la voce **Rimuovi queste impostazioni**.
3. Per modificare le opzioni del processo, sceglierlo nella lista dei processi. In questo caso si apre la finestra **Editor dei task**, descritta sotto.
4. Per aggiungere un compito nella lista, scegliere nella barra degli strumenti la voce **Nuovo task**. In questo caso si apre la finestra **Nuovo task**, uguale a **Editor dei task**. Indicare i parametri necessari (v. sotto) e premere sul tasto **Salva**.

5. Si possono bloccare l'esecuzione del processo o consentire l'esecuzione del processo bloccato in precedenza.
6. Per esportare l'orario nel file del formato speciale, premere sul tasto nella barra degli strumenti.
7. Per importare i parametri da questo file, premere sul tasto nella barra degli strumenti.



Valore dei campi, marcati con il carattere *, sono obbligatori da impostare.

### *Per modificare i parametri del processo:*

1. Nella scheda **Generali** impostare i seguenti parametri:
   - Inserire nel campo **Nome** il nome del processo, con cui viene visualizzato nell'orario.
   - Per attivare l'esecuzione del processo, mettere il flag **Permettere l'esecuzione**.

   Se il flag non è attivo, il processo è presente nella lista, ma non viene eseguito.
   - Il flag attivo **Task critico** indica di eseguire il processo all'avvio successivo di **Enterprise Server**, se l'esecuzione di tale processo viene saltata da (**Enterprise Server** è disconnesso al momento di esecuzione del processo). Se in un certo periodo il processo è saltato più volte, all'avvio di **Enterprise Server** viene eseguito una volta sola.
2. Nella scheda **Azione** scegliere nella lista a cascata **Azione** il tipo di processo. In questo caso si cambia l'aspetto della parte inferiore della finestra, che contiene i parametri supplementari di questo tipo di processo. Inserire questi parametri (in tabella 8-3 i parametri di processi sono analizzati separatamente per tipi).
3. Nella scheda **Tempo** nella lista a cascata **Tempo** scegliere la periodicità di avvio del processo e impostare l'ora secondo la periodicità scelta (questa azione è simile all'impostazione del tempo nell'orario di workstation, v. sopra Configurazione orario processi su workstation).
4. Premere sul tasto **Salva**.

**Tabella 8-3. Tipi di processi e i loro parametri**

| Tipo processo | Parametri e descrizione |
|---|---|
| Procedura in esecusione | Si deve indicare il nome della procedura eseguita nel campo **Nome**. Il nome della procedura deve corrispondere al nome dello script lua dell'utente eseguito (senza estensione), locato nella cartella `var/extensions` della cartella di installazione del Server (v. anche la descrizione degli script dalla cartella `var/extensions`, riportata in Allegato M). |
| Chiusura | Per completare l'operazione del Server. Non ha parametri supplementari. |
| Riavvio | Per riavviare il Server. Non ha parametri supplementari. |
| Avvio | Si deve indicare nel campo **Percorso** il percorso al file eseguibile del programma, eseguita attualmente, nel campo **Argomenti** – parametri della riga di comando per avviare il programma indicato. Mettere il flag **Eseguire sincronicamente** per la sincronizzazione con il **Server** – aspettare il completamento di esecuzione di questo programma prima di eseguire altri processi tipo **Avvio**. Se il flag **Eseguire sincronicamente** non è attivo, il **Server** avvia il programma e registra solo il suo avvio. Se il flag **Eseguire sinconicamente** è attivo, il **Server** registra il suo avvio, il codice di ritorno e il tempo di terminazione del programma. |
| Ricordo della scadenza della licenza | Si deve indicare il periodo, entro cui sarà ricevuto l'avviso sulla scadenza del periodo di validità di licenza del prodotto **Dr. Web** (sia di licenza del **Server**, sia di **Agent**). |
| Aggiornamento | Sul processo v. Aggiornamento programmato. |
| Log | Si deve indicare il testo dell'avviso da inserire nel log. |
| Copie di reserva dei dati critici del server | I processi sono destinati a creare il backup dei dati critici del **Server** (database, file della chiave di licenza del Server, chiave di codifica chiusa). Si deve indicare il percorso alla cartella, dove verranno salvati i dati (percorso vuoto significa cartella predefinita) e il numero massimo di backup (valore 0 significa togliere questa limitazione). Per più informazioni v. Allegato H5.5. |

| Tipo processo | Parametri e descrizione |
|---|---|
| La postazioni non ha visitato il server da molto tempo | Si deve indicare il periodo, a cui scandenza workstation è considerata non accessa a lungo al **Server**, e ne verrà visualizzato un avviso. |
| Rimozione degli eventi non inviati | Si deve indicare il periodo, a cui scadenza gli eventi non inviati verranno eliminati. Qui si intendono eventi, passati dal **Server** slave al master. Se la trasmissione fallisce, l'evento viene aggiunto alla lista di non inviati. Il **server** slave con la periodicità impostata esegue i tentativi di trasmissione. Con l'esecuzione del processo **Rimozione degli eventi non inviati** viene eseguita l'eliminazione di tutti gli eventi, la cui durata di conservazione ha raggiunto e ha superato il periodo impostato. |
| Rimozione delle postazioni vecchie | Si deve indicare il periodo di tempo (di default 90 giorni).<br>Le workstation, che non hanno accesso al **Server** durante il periodo indicato, sono considerate vecchie e vengono eliminate dal **Server**. |
| Rimozione delle registrazioni vecchi | Si deve indicare il numero di giorni, a cui scadenza i dati statistici su workstation (non workstation stesse) si definiscono vecchi e vengono eliminati dal **Server**.<br>Il periodo di eliminazione di dati statistici è impostato separatamente per ogni tipo di record. |



I dati vecchi vengono automaticamente eliminati dal database per risparmiare lo spazio sul disco. Il periodo predefinito per **Rimozione delle registrazioni vecchi** e **Rimozione delle postazioni vecchie** è di 90 giorni. Diminuzione di tale parametro comporta la rilevanza minore delle statistiche accumulate dell'operazione dei componenti della rete antivirus. Aumento del parametro potrebbe aumentare notevolmente la richiesta di risorse dal Server.

# 8.4. Gestione repositorio di Dr.Web Enterprise Server

## 8.4.1. Introduzione

*Il repositorio di* **Enterprise Server** è destinato a conservare i campioni modelli del software e al loro aggiornamento dai server di **SAM**.

A questo scopo il repositorio opera con i set di file, chiamati *prodotti*. Ogni prodotto è messo nella sottocartella separata della cartella `repository`, locata nella cartella `var`, il che, con installazione predefinita, è la sottocartella della cartella radice del **Server**. Le funzioni di repositorio e la loro gestione vengono eseguite per ogni prodotto indipendentemente.

Per gestire aggiornamento il repositorio utilizza il concetto di edizione del prodotto. L'edizione è lo stato corretto ad un certo periodo del tempo dei file di prodotto (compende i nome dei file e gli importi di controllo) ed è caratterizzata dal numero unico. Il repositorio esegue la sincronizzazione delle edizioni del prodotto nei seguenti direzioni:

a) su **Enterprise Server** dal sito di aggiornamento del prodotto (via protocollo HTTP),



Per le versioni del **Server 5.0** e superiori, nonostante le impostazioni del repositorio per il software del **Server**, gli aggiornamenti dai server di **SAM** non sono forniti.

Per aggiornamento del **Server** utilizzare l'installazione della versione richiesta ed eseguire la procedura dell'aggiornamento a secondo delle regole comuni, riportate nelle sezioni Aggiornamento di Dr.Web ESS per il SO Windows® o Aggiornamento di Dr.Web ESS per i SO della famiglia UNIX®.

b) tra vari **Enterprise Server** nella configurazione multiserver (a seconda della politica di scambio impostata),

c) da **Enterprise Server** su workstation.

Il repositorio permette all'Amministratore della rete antivirus di impostare i seguenti parametri:

- lista dei siti di aggiornamento nelle operazioni del tipo **a)**;
- limitazione composizione dei prodotti che richiedono la sincronizzazione del tipo **a)** (in questo modo, l'utente ha la possibilità di tracciare solamente le modifiche che necessita delle categorie singole dei prodotti);
- limitazione dei parti di prodotti, che non richiedono la sincronizzazione del tipo **c)** (utente può scegliere, che cosa concretamente è da installare su workstation);
- il controllo di passaggio alle edizioni nuove (si possono testare i prodotti per conto proprio prima dell'implementazione);
- di aggiungere in prodotti i propri componenti;
- di creare indipendentemente degli nuovi prodotti, per cui anche viene eseguita la sincronizzazione.

Attualmente nella fornitura sono compresi i seguenti prodotti:

- **Enterprise Server**,
- **Enterprise Agent** (software di **Agent**, software antivirus di workstation),
- **Centro gestione** di **Dr.Web**,
- Database dei virus.

Per più informazioni sul repositorio v. Allegato F. Gestione repositorio.

## 8.4.2. Stato del repository

Per controllare lo stato attuale del repositorio o aggiornare i componenti della rete antivirus, scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Stato del repository**.

Nella finestra aperta c'è la lista dei componenti della rete antivirus, la loro data di ultimo aggiornamento e il loro stato attuale.

Per verificare la disponibilità di aggiornamenti e scaricare i disponibili aggiornamenti di componenti dai server **SAM** premere il tasto **Verifica aggiornamenti**.

## 8.4.3. Editor configurazioni del repository

Editor di configurazioni del repositorio permette di impostare i parametri generali di configurazione del repositorio per tutti i prodotti.



Dopo che le configurazioni del repositorio sono modificate, si deve completare con successo l'aggiornamento del software dei componenti di rete antivirus per modificare lo stato del repositorio secondo le configurazioni scelte.

Per modificare la configurazione del repositorio, scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Configurazione del repository**.

## Configurazione SAM Dr.Web

Nella scheda **SAM Dr.Web** si esegue la configurazione dei parametri del **Sistema aggiornamenti mondiale**.

***Con il Centro gestione di Dr.Web si può:***

- Eliminare server dalla lista. Per farlo, scegliere uno o più server e nella barra degli strumenti premere sul tasto **Rimuovi i server dalla lista**  .



Per scelgiere più server contemporaneamente, utilizzare i tasti CTRL o SHIFT.

- Aggiungere server alla lista. Per farlo, nella barra degli strumenti premere sul tasto **Crea server**  e impostare le configurazioni del server secondo la procedura, riportata sotto.

- Impostare server proxy. Per farlo, mettere il flag **Usa server proxy** (le configurazioni di proxy sono analoghi alle configurazioni dei server di aggiornamenti).
- Configurare indirizzo server e i parametri di autorizzazione dell'utente. Per farlo, premere su icona del server.

Quando si crea o si aggiunge un server, si apre la finestra di configurazioni del server.

***Per impostare le configurazioni del server di aggiornamenti:***

1. Premere su icona del server corrispondente.
2. Nei campi di input **Server** indicare rispettivamente l'indirizzo e la porta del Server.
3. Nei campi **Utente** e **Password** si può impostare nome utente e password sul server di aggiornamenti. Se l'autorizzazione sul server non è richiesta, lasciare questi campi vuoti.
4. Per salvare le configurazioni modificate, premere sul tasto **Salva**.

Si può inoltre impostare l'accesso a tutti server di aggiornamenti via un server proxy.

***Per aggiungere un server proxy:***

1. Mettere il flag **Utilizzare server proxy**.
2. Nella finestra aperta di configurazioni del server proxy impostare i parametri, analoghi ai parametri del server di aggiornamenti.
3. Premere sul tasto **Aggiungi.**
4. Premere sul tasto **Salva**.



Durante la configurazione del server proxy si deve prestare attenzione soprattutto al tipo di autorizzazione utilizzata.

Nella versione corrente di **Dr.Web Enterprise Security Suite** è supportata solo l'autorizzazione HTTP di base, l'autorizzazione HTTP proxy e l'autorizzazione RADIUS.

Se si devono disconnettere i server di aggiornamenti dal server proxy, togliere il flag **Usa server proxy**.

## Configurazione aggiornamenti di Dr.Web Enterprise Agent

Configurazione di aggiornamento del repositorio per il software di **Agent** e il pacchetto antivirus è configurata separatamente per varie versioni dei SO, su cui sarà installato tale software:

- Nella scheda **Dr.Web Enterprise Agent per Windows** nel gruppo di tasti di scelta indicare, se si richiede l'aggiornamento di tutti i componenti, installati su workstation nel SO Windows, o solo dei database dei virus.
- Nella scheda **Dr.Web Enterprise Agent per Unix** nel gruppo di tasti di scelta indicare, per quali SO della famiglia UNIX si richiede l'aggiornamento dei componenti, installati su workstation.

## Configurazione aggiornamenti di Dr.Web Enterprise Server

Nella scheda **Dr.Web Enterprise Server** nel gruppo di tasti di scelta si indica, per quali SO si richiede l'aggiornamento dei file del **Server**: una parte per il SO Windows, una parte per il SO UNIX, tutte e due le parti o nessuna.



Per le versioni del **Server 5.0** e superiori, nonostante le configurazioni di tale sezione, aggiornamenti dai server **SAM** non sono forniti.

Per aggiornare il **Server**, utilizzare l'installazione della versione richiesta ed eseguire la procedura di aggiornamento secondo le regole generali, riportate nelle sezioni Aggiornamento di Dr.Web ESS nei SO Windows® o Aggiornamento di Dr.Web ESS nei SO della famiglia UNIX®.

# 8.5. Particolarità di rete con più server di Dr.Web Enterprise Server

**Dr.Web Enterprise Security Suite** permette di creare rete antivirus con più **Enterprise Server**. In questo caso ogni workstation viene ascritta a un **Server** concreto, il che permette di distribuire il carico tra di loro.

Le connessioni tra i **Server** possono avere la struttura gerarchica, che permette di distribuire il carico su **Server** nel modo ottimale.



Alla pianificazione della struttura della rete antivirus si devono prendere in considerazione le particolarità di fornitura delle licenze per la rete con più **Server**. Per più informazioni v. File della chiave.

Per lo scambio dell'informazione tra i **Server** (aggiornamenti dei file di componenti e dati del funzionamento di **Server** e di workstation connesse ad essi) si utilizza il *protocollo di sincronizzazione intraserver* speciale.

La più importante proprietà di questo protocollo è l'operatività di trasmissione di aggiornamenti.

***Con questo protocollo:***

- aggiornamenti vengono passati appena ricevuti,
- non è necessario configurare l'orario di aggiornamento del **Server** (oltre i **Server**, che ricevono aggiornamenti dai server **SAM** di **Dr.Web**, utilizzando il protocollo HTTP).

## 8.5.1. Struttura di rete con più Dr.Web Enterprise Server

Nella rete antivirus si possono installare più **Enterprise Server**. In questo caso ogni **Enterprise Agent** si connette a uno dei **Server**.

Ogni **Server** insieme a workstation antivirus connesse opera come una rete antivirus separata, come descritto nelle sezioni precedenti.

**Dr.Web Enterprise Security Suite** permette di connettere tali reti antivirus, organizzando la trasmissione di informazione tra **Enterprise Server**.

***Dr.Web Enterprise Server può passare a un'altro Dr.Web Enterprise Server:***

- aggiornamenti del software e di database dei virus. In questo caso riceve gli aggiornamenti dai server **SAM** di **Dr.Web** solo uno di essi;



Si consiglia di aggiungere all'orario di **Enterprise Server** slave il processo di aggiornamento di **Enterprise Server** slave dai server **SAM** nel caso il **Server** master sia provvisoriamente non raggiungibile. Questo permette ad **Agent** di ottenere gli aggiornamenti di database dei virus e dei plugin di programma (v. anche Editor configurazione repositorio).

- informazioni sulle statistiche dei virus, statistiche di operazione ecc.

***Dr.Web Enterprise Security Suite distingue due tipi di rapporti tra Dr.Web Enterprise Server:***

- *rapporto del tipo master-slave*, in cui master passa a slave gli aggiornamenti e riceve le informazioni su eventi,
- *rapporto tra pari*, in cui le direzioni di informazioni passate e i tipi di essa sono personalizzate.

In immagine 8-1 è rappresentata una struttura di rete con più **Server**.

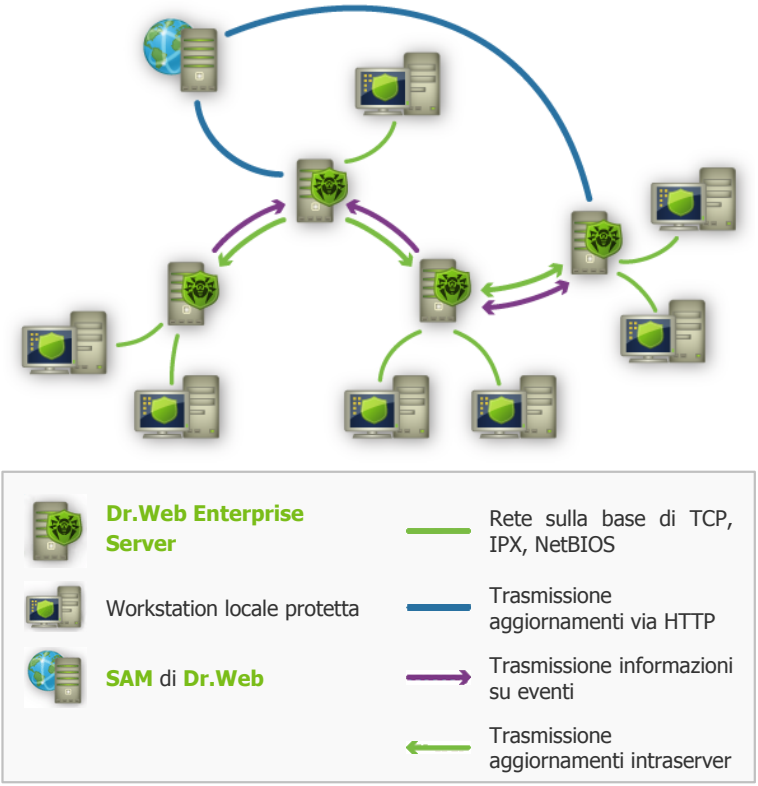



**Immagine 8-1. Rete con più Server**

***Alcuni vantaggi di rete antivirus con più Dr.Web Enterprise Server sono:***

- possibilità di ottenere aggiornamenti dai server **SAM** di **Dr.Web** tramite un **Enterprise Server** con trasmissione successiva ad altri **Server** direttamente o via altri intermediari,
- possibilità di distribuire workstation su più **Server**, diminuendo il carico su ognuno di essi,
- unione delle informazioni da più **Server** su uno; possibilità di ottenere tali informazioni nella sessione del **Centro gestione** su questo **Server** nel modo consolidato.



**Dr.Web Enterprise Security Suite** autonomamente traccia e non consente i percorsi ciclici di trasmissione delle informazioni.

## 8.5.2. Configurazione comunicazioni intra-server tra Dr.Web Enterprise Server

Per utilizzare la possibilità di operazione con più **Server**, si deve configurare la comunicazione tra di essi.

Si consiglia di programmare preliminariamente e disegnare la struttura di rete antivirus, marcando tutti i flussi di informazione presupposti e prendendo decisione su quali comunicazioni saranno "tra pari", e quali - del tipo "principale-ausiliare". Dopodiché per ogni **Server** che fa parte di rete, si deve configurare la comunicazione con un **Server** "vicino", cioè con quale è connesso con almeno un flusso di informazione.

***Esempio di configurazione di comunicazione dei server Dr.Web Enterprise Server principale e ausiliario:***



I valori dei campi, marcati con il carattere *, sono obbligatori da impostare.

1. Assicurarsi che tutti e due **Enterprise Server** operano correttamente.
2. Assicurarsi che ogni **Enterprise Server** ha la chiave `enterprise.key` diversa.
3. Con il **Centro gestione** connettersi a ogni **Enterprise Server** e darli nomi "parlanti", il chè permette di non sbagliare durante le operazioni, necessarie per connettere **Enterprise Server** e per la loro gestione. Si può farlo nel menu del **Centro gestione** **Amministrazione** → **Configurazione Dr.Web Enterprise Server** nella scheda **Generali** nel campo **Nome**. In questo esempio chiamiamo il **Server**

principale `MAIN`, e supplementare (che sarà ausiliario) – `AUXILIARY`.

4. Attivare su tutti e due **Enterprise Server** il protocollo di server. Per farlo, nel menu del **Centro gestione** **Amministrazione** → **Configurazione di Dr.Web Enterprise Server** nella scheda **Moduli** mettere il flag **Dr.Web Enterprise Server** (v. Configurazione di Dr.Web Enterprise Server).



Se il protocollo di server non è attivo, durante la creazione di una nuova connessione nel **Centro gestione** si visualizza l'avviso di necessità di attivazione di tale protocollo e si indica il link alla sezione corrispondente del **Centro gestione**.

5. Riavviare tutti e due **Enterprise Server**.
6. Connettere il **Centro gestione** al **Server** ausiliario `(AUXILIARY)` e aggiungere un **Server** principale `(MAIN)` alla lista dei **Server** vicini del **Server** ausiliario. Per farlo, scegliere la voce **Legami** nel menu principale. Si apre la finestra che contiene la lista gerarchica dei **Server** della rete antivirus. Per aggiungere un **Server** a questa lista premere sul tasto **Crea una relazione**  nella barra degli strumenti.

   Si apre la finestra di descrizione di comunicazione di **Server** attuale e di quello aggiunto (v. immagine 8-2). Scegliere il tipo **Principale**. Nel campo **Nome** inserire il nome del **Server**principale `(MAIN)`, nel campo **Password** inserire una password per accedere al **Server** principale. A destra del campo **Chiave** premere sul tasto **Sfogliare** e indicare la chiave `drwcsd.pub`, relativa al **Server** principale, e nel campo **Indirizzo** inserire l'indirizzo del **Server** principale.

   Si può ricercare la lista dei **Server**, disponibili in rete. Per farlo:

   a) Premere la freccia a destra del campo **Indirizzo**.

b) Nella finestra aperta indicare la lista delle reti nel formato: separate da trattino (per esempio, `10.4.0.1-10.4.0.10`), separate da virgola e spazio (per esempio, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`), utilizzando il prefisso di rete (per esempio, `10.4.0.0/24`).

c) Premere sul tasto  . Parte la ricerca di rete per la presenza dei **Server** disponibili.

d) Scegliere un **Server** nella lista dei **Server** disponibili. Il suo indirizzo sarà scritto nel campo **Indirizzo** per creare una connessione.

Nel campo **Indirizzo della console di amministrazione** si può indicare l'indirizzo di pagina iniziale del **Centro gestione** per **Server** principale (v. Centro gestione Dr.Web).

I flag nelle sezioni **Aggiornamenti** e **Eventi** sono posti secondo il principio di comunicazione *principale-ausiliario* e non si possono modificare:

- **Server** principale invia aggiornamenti ai **Server** ausiliari;
- **Server** principale riceve le informazioni su eventi dai **Server** ausiliari.

Premere sul tasto **Salva**.

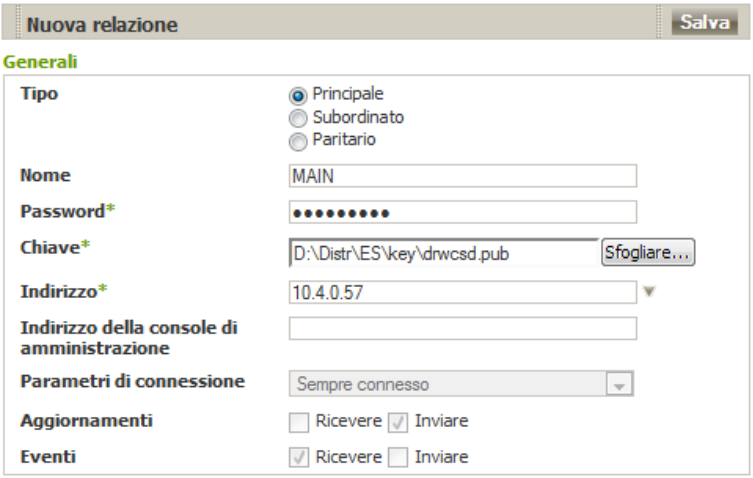



**Immagine 8-2.**

Come risultato il **Server** principale (`MAIN`) entra nelle cartelle **Principali** e **Offline** (v. immagine 8-3).

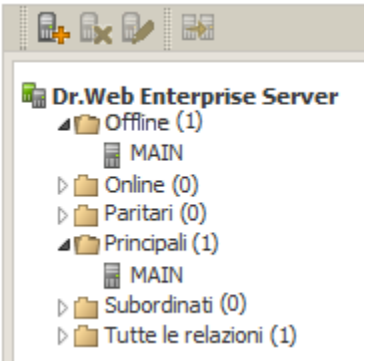



**Immagine 8-3.**

7. Connettere il **Centro gestione** al **Server** principale (`MAIN`) e aggiungere un **Server** ausiliario (`AUXILIARY`) alla lista dei **Server** vicini del **Server** principale. Per farlo, scegliere la voce **Legami** nel menu principale. Si apre la finestra, che contiene la lista gerarchica dei **Server** della rete antivirus, "vicini" al

Server attuale. Per aggiungere un **Server** a questa lista premere sul tasto **Crea una relazione** nella barra degli strumenti.

Nella finestra aperta (v. immagine 8-4) scegliere il tipo **Subordinato**. Nel campo **Nome** inserire il nome del **Server** ausiliario (`AUXILIARY`), nel campo **Password** inserire la stessa password di quella indicata nella voce **6.** A destra del campo **Chiave** premere sul tasto **Sfogliare** e indicare la chiave `drwcsd.pub`, relativa al **Server** ausiliario.

Nel campo **Indirizzo della console di amministrazione** si può indicare l'indirizzo di pagina iniziale del **Centro gestione** per **Server** ausiliario (v. Centro gestione di Dr.Web).

I flag nelle sezioni **Aggiornamenti** e **Eventi** sono posti secondo il principio di comunicazione *principale-ausiliario* e non si possono modificare:

- **Server** ausiliario riceve aggiornamenti dal **Server** principale;
- **Server** ausiliario invia le informazioni su eventi al **Server** principale.

Premere sul tasto **Salva**.




**Immagine 8-4.**

Come risultato il **Server** ausiliario (AUXILIARY) entra nelle cartelle **Subordinati** e **Offline** (v. immagine 8-5).

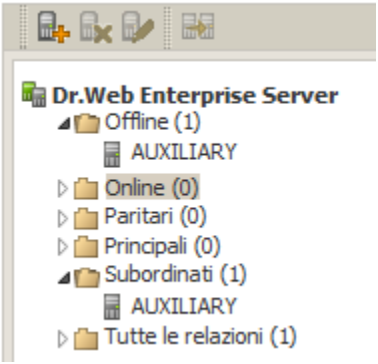



**Immagine 8-5.**

8. Aspettare che si stabilisca la connessione tra i **Server** (di solito ci vuole meno di un minuto). Per il controllo aggiornare periodicamente la lista dei **Server** con il tasto F5. Appena stabilita una connessione, il **Server** ausiliario (AUXILIARY) passa dalla cartella **Offline** alla cartella **Online** (v.

immagine 8-6).

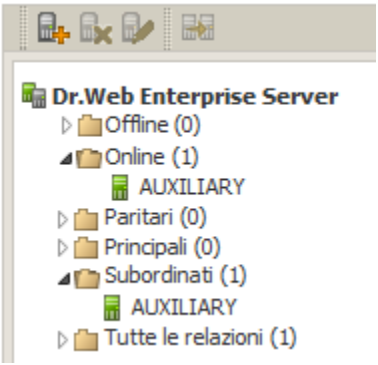



**Immagine 8-6.**

9. Connettere il **Centro gestione** al **Server** ausiliario (`AUXILIARY`) e assicurarsi che il **Server** principale (`MAIN`) è connesso all'ausiliario (`AUXILIARY`) (v. immagine 8-7).

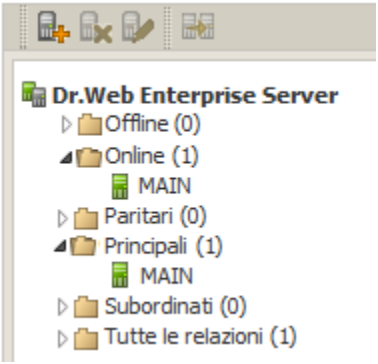



**Immagine 8-7.**



Non si possono connettere due **Server** con la stessa chiave di licenza (`enterprise.key`).

Non si possono connettere più **Server** con la stessa copia dei parametri: password e chiave di codifica aperta `drwcsd.pub`.



Durante la creazione di comunicazione "alla pari" intraserver, si consiglia di indicare l'indirizzo del **Server** connesso nelle configurazioni di solo uno di essi.

Questo non influisce su interazione tra i **Server**, però permette di evitare le scritture del tipo **Link with the same key id is already activated** nel protocollo di operazione del **Server**.

***Non si può stabilire una connessione tra Dr.Web Enterprise Server nei seguenti casi:***

- Problemi connessioni di rete.
- Alla configurazione di comunicazione è stato impostato un indirizzo sbagliato del **Server** principale.
- È stata impostata chiave di codifica aperta scorretta `drwcsd.pub` su uno dei **Server**.
- È stata impostata password di accesso scorretta su uno dei **Server** (sono impostate le password non corrispondenti su **Server connessi**).
- Stessa chiave di licenza `enterprise.key` su tutti e due dei **Server**.
- Chiave di licenza `enterprise.key` di **Server** ausiliario connessa è la stessa del **Server** ausiliario, già connessa allo stesso **Server** principale.



Durante la creazione di comunicazioni tra **Server** si può impostare delle limitazioni di aggiornamenti per i **Server** connessi. Per farlo, alla creazione di comunicazione, nella barra **Limitazioni di aggiornamenti** premere sul tasto. Si apre la finestra di modifica delle modalità di aggiornamento, descritta in Limitazione aggiornamenti.

## 8.5.3. Utilizzo di rete antivirus con più Dr.Web Enterprise Server

Una particolarità di rete con più **Server** è l'ottenimento di aggiornamenti dai server **SAM** di **Dr.Web** via una parte di **Enterprise Server** (di solito, uno o più **Server** master). In questo caso solo su questi **Server** si deve impostare l'orario, che contiene il processo di aggiornamento (v. Configurazione orario di Dr.Web Enterprise Server). Qualsiasi **Server** che ha ottenuto degli aggiornamenti dai server **SAM** di **Dr.Web** o da un altro **Server**, lo passa immediatamente a tutti i **Server**, per cui tale possibilità è configurata su di esso (cioè a tutti i slave connessi, nonché a quelli dello stesso livello, su cui è esplicitamente impostata la possibilità di ottenere degli aggiornamenti).



**Dr.Web Enterprise Security Suite** traccia automaticamente le situazioni, quando per la programmazione incorretta della topologia della rete e della configurazione dei **Server** sullo stesso **Server** di nuovo arriva un aggiornamento già ottenuto da un'altra fonte, e non esegue l'aggiornamento di nuovo.

L'amministratore può inoltre ottenere le informazioni consuntive sugli eventi dei virus più importanti nei segmenti della rete, connesse a qualche **Server** via le connessioni intraserver (per esempio, nella configurazione descritta sopra "un master, altri slave" questa informazione è consolidata sul **Server** principale).

***Per visualizzare le informazioni su eventi dei virus su tutti i Dr.Web Enterprise Server, connesse a questo:***

1. Scegliere la voce **Connessioni** del menu principale del **Centro gestione**.
2. Nella finestra aperta nella sezione del menu di gestione **Tabelle** scegliere la voce **Report compositio** nella finestra aperta nella sezione del menu di gestione **Tabelle** scegliere la voce **Report compositio** per visualizzare le informazioni sulla quantità totale di record di eventi dei **Server** vicini. Nella tabella con le statistiche dei **Server** vicini si visualizzano i dati delle seguenti sezioni:

- **Infezioni** - infezioni, rilevati su workstation, connesse ai **Server** vicini.
- **Errori** - errori di scansione.
- **Statistiche** - statistiche delle infezioni rilevate.
- **Avvio/Terminazione** - avvio e completamento dei processi di scansione di workstation.
- **Stato** - stato del software antivirus sulle workstation.
- **Tutte le installazioni di rete** - installazioni di rete di **Agent**.

3. Per passare alla pagina delle tabelle con le informazioni più dettagliate su eventi dei **Server** vicini, premere sul numero nella tabella della sezione **Report compositio** con il numero di record su evento richiesto.
4. Inoltre per passare alla tabella di dati su eventi dei **Server** vicini, scegliere la voce corrispondente (v. passo 2) della sezione **Tabelle** del menu di gestione.
5. Per visualizzare i dati per un certo periodo indicare il range del tempo rispetto al giorno odierno dalla lista a cascata o impostare un range dei dati nella barra degli strumenti. Per impostare un range, inserire le date richieste o premere sulle icone del calendario accanto ai campi di date. Per visualizzare i dati premere sul tasto **Aggiorna**.
6. Se è necessario salvare la tabella per la stampa o per un'ulteriore elaborazione, premere nella barra degli strumenti sul tasto  **Registra le informazioni in un file del formato CSV,** sul tasto  **Registra le informazioni in un file del formato HTML** o sul tasto  **Registra le informazioni in un file del formato XML**.

## 8.5.4. Operazione di più Server Dr.Web Enterprise Server con database unico

Alla creazione di rete antivirus con più **Enterprise Server** e con un database unico si devono eseguire le seguenti prescrizioni:

1. Su tutti i **Server** devono essere uguali le chiavi di codifica `drwcsd.pub`, `drwcsd.pri`, i certificati `certificate.pem`, `private-key.pem` e la chiave di agent `agent.key`.
2. Nel file di configurazione del **Centro gestione** `webmin.conf` per tutti i **Server** deve essere identificato lo stesso nome DNS del **Server** nel parametro `ServerName`.
3. Sul server DNS in rete viene registrato il nome comune di cluster per ogni singolo **Server** e viene impostato il metodo di bilanciamento del carico.
4. Ogni **Server** deve avere la propria chiave `enterprise.key` con l'identificatore unico `ID1`.
5. Nei file di configurazione dei **Server** `drwcsd.conf` per tutti i **Server** deve essere definito un database esterno.
6. Nell'orario di server i processi **Purge Old Data**, **Prepare and send fiscal report periodic job**, **Backup sensitive data**, **Purge old stations**, **Purge expired stations**, **Purge old data**, **Purge unsent IS events** devono essere impostati solo su uno dei **Server** (il più produttivo, se le configurazioni sono diverse).

# Capitolo 9. Aggiornamento di Dr.Web Enterprise Security Suite e di componenti singoli



Prima di iniziare l'aggiornamento di **Dr.Web ESS** e dei componenti singoli di esso si consiglia di controllare la correttezza delle impostazioni del protocollo TCP/IP per poter accedere ad Internet. In particolare, il servizio DNS deve essere attivo e avere le impostazioni corrette.

Aggiornamento delle basi di dati dei virus e del software può essere eseguito sia manualmente, sia con task manager di **Server** e di **Agent.**



Prima di aggiornare il software si consiglia di configurare il repositorio, compreso accesso a **SAM** di **Dr.Web** (v. Editore di configurazione di repositorio).

## 9.1. Aggiornamento di Dr.Web Enterprise Security Suite

### 9.1.1. Aggiornamento di Dr.Web Enterprise Server per i SO Windows®

Sono possibili due varianti di aggiornamento del software di **Server** fino alla versione **6.0.4:**

1. Aggiornamento automatico. L'aggiornamento del **Server** dalle versioni **5.0** e **6.0.0** viene eseguito in modo automatico tramite programma di installazione.



L'aggiornamento automatico è possibile solamente per i **Server** che hanno lo stesso numero di bit.

Nel caso contrario si deve rimuovere il **Server** vecchio e installare il **Server** nuovo manualmente.

2. Aggiornamento manuale. All'aggiornamento del **Server** dalle versioni **4.XX**, **6.0.2** e superiore si deve rimuovere il **Server** precedente manualmente e installare il **Server** nuovo.

## *Salvataggio dei file di configurazione*

All'eliminazione manuale del **Server** e all'aggiornamento del **Server** via programma di installazione, i seguenti file vengono salvati automaticamente:

| File | Descrizione | Cartella predefinita |
|---|---|---|
| `dbinternal.dbs` | database interno | `var` |
| `drwcsd.conf` (nome può essere diverso) | file di configurazione del **Server** | `etc` |
| `drwcsd.pri` | chiave di codifica chiusa | |
| `drwcsd.pub` | chiave di codifica aperta | • `Installer`<br>• `webmin\install` |
| `enterprise.key` (nome può essere diverso) | chiave di licenza di **Server** | `etc` |
| `agent.key` (nome può essere diverso) | chiave di licenza di **Agent** | |
| `certificate.pem` | certificato per SSL | |
| `private-key.pem` | chiave chiusa RSA | |

Se è necessario, altri file importanti si possono salvare in altro posto, diverso dalla cartella di installazione del **Server**, per esempio, il file di configurazione del **Centro gestione** `webmin.conf` e i moduli dei

log, che si trovano nella cartella `\var\templates`.

## Salvataggio della base di dati

Prima di aggiornare il software **Dr.Web Enterprise Security Suite**, si raccomanda di eseguire copiatura di riserva della base di dati.

***Per salvare la base di dati:***

1. Arrestare il **Server**.
2. Esportare la base di dati nel file:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe"    -home="C:\Program    Files\DrWeb
Enterprise Server" -var-root="C:\Program Files
\DrWeb Enterprise Server\var" -verbosity=all
exportdb <cartella_copia_backup>\esbase.es
```

In caso dei **Server** che utilizzano base di dati esterna, si raccomanda di utilizzare strumenti standard, forniti insieme alla base di dati.



Assicurarsi che l'esportazione della base di dati di **Dr.Web ESS** si sia completata con successo. L'assenza di una copia di riserva della base di dati non farà possibile ripristinare il **Server** in caso di emergenza.

## Note importanti



Partendo dalla versione **5.0**, nel pacchetto antivirus di **Dr.Web Enterprise Security Suite** sono inclusi i prodotti **SpIDer Gate** e **Controllo Ufficio**, per poter utilizzare i quali è necessario che essi siano indicati nella licenza **(Antivirus+Antispam)**. Se tali prodotti non sono indicati nella licenza, si consiglia di eseguire le azioni sottostanti.

Se sul computer con **Enterprise Server** è installato **Agent** con l'auto-protezione attiva, nel processo di aggiornamento del **Server** sarà visualizzato il messaggio sull'operazione del componente di auto-protezione **Dr.Web SelfPROtect.** Per procedere all'aggiornamento del software del **Server**, disattivare tale componente via impostazioni di **Agent**.

Se come database esterno si utilizza ODBC per Oracle, all'aggiornamento (o alla installazione reiterata) del **Server**, nelle impostazioni del programma di installazione scegliere la voce Installazione **Personalizzata** e nella finestra successiva annullare l'installazione del client integrato per DBMS Oracle (nella sezione **Database support** - **Oracle database driver**).

Nel caso contrario l'operazione con il database Oracle via ODBC non sarà possibile per il conflitto di librerie.

## Aggiornamento automatico di Dr.Web Enterprise Server dalle versioni 5.0 e 6.0.0

Aggiornamento del software del **Server** della versione **5.0** e **6.0.0** fino alla versione **6.0.4** viene eseguito automaticamente dagli strumenti del programma di installazione.

***Per aggiornare Dr.Web Enterprise Server avviare il programma di installazione e seguire le indicazioni dell'installazione guidata:***

1. Nell'aggiornamento sarà visualizzata la finestra **Dr.Web Enterprise Server commenti all'aggiornamento**, che avverte della presenza del software del **Server** della versione precedente installato. Programma di installazione automaticamente definisce la cartella di installazione del **Server**.
2. Nei passi successivi dell'installazione guidata viene visualizzata l'informazione sui percorsi ai file del **Server** della versione precedente (v. sopra), che saranno utilizzati dal programma di installazione all'installazione del **Server** della versione **6.0.4**. Se necessario, i percorsi ai file, trovati automaticamente dal programma di installazione, si possono modificare.

3. Per procedere a eliminare il **Server** della versione precedente e a installazione del **Server** della versione **6.0.4** cliccare il pulsante **Installare**.



Nel processo di aggiornamento del software del **Server** i contenuti del repositorio vengono eliminati e si installa una versione nuova.

Se per qualche motivo si sia salvato il repositorio della versione precedente, si devono manualmente eliminare tutti i contenuti del repositorio e eseguirne l'aggiornamento completo.

Se la rete antivirus ha una configurazione a più server, solo le basi di dati dei virus verranno trasmesse dal **Server** master dalla versione **6.0.4** ai **Server** slave dalla versione **5.0** e inferiore.

Per passare gli aggiornamenti di tutto il software antivirus, si deve aggiornare il **Server** slave fino alla versione **6.0.4** (per compatibilità di struttura dei repositori).

***Dopo l'aggiornamento di Dr.Web Enterprise Server alla versione 6.0.4 si consiglia di eseguire le seguenti azioni:***

Dopo l'aggiornamento del software di **Dr.Web Enterprise Server** secondo lo schema generale si devono eseguire le seguenti azioni, necessarie per il funzionamento regolare del **Centro gestione**:

1. Cancellare la cache del browser web, utilizzato per connessione al **Centro Gestione**.
2. Aggiornare il plug-in **Dr.Web Browser-Plugin**.

## Aggiornamento manuale di Dr.Web Enterprise Server dalle versioni 4.XX, 6.0.2 e superiore

Non si supporta l'aggiornamento del software **Server** dalle versioni **4.XX**, **6.0.2** e superiore tramite programma installazione di **Enterprise Server 6.0.4**. Per passare alla versione **6.0.4,** è necessario rimuovere manualmente il **Server** installato e installare il **Server** nuovo.



Nel caso di aggiornamento dalla versione **4.xx**, se nella licenza del software antivirus della versione **6.0.4** non sono specificati i prodotti **SpIDer Gate** e **Ufficio Control (Antivirus+Antispam)**, si raccomanda di eseguire le azioni descritte sotto.

***Per aggiornare Dr.Web Enterprise Server eseguire le seguenti azioni:***

1. Arrestare **Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).
2. Se si utilizza un database esterno, salvare il database con strumenti del server SQL.
3. Se si vuole utilizzare ulteriormente qualche file (oltre i file, che saranno salvati automaticamente nel processo di eliminazione del **Server**), creare manualmente le copie di riserva di tali file, per esempio, i moduli del log ecc.
4. Eliminare **Server**.
5. Installare un **Server** nuovo (v. Installazione di Dr.Web Enterprise Server per i SO Windows®). All'installazione del **Server** impostare nei parametri del programma di installazione i file salvati automaticamente.

   Se si utilizza database esterno, indicare creazione di un database nuovo.

   Se si utilizza database interno, indicare il file del database salvato `dbinternal.dbs`.

6. Arrestare il **Server** (v. Avvio e arresto di Dr.Web Enterprise Server).
7. Se prima di eliminare il **Server** sono stati salvati manualmente alcuni file, metterli nelle stesse cartelle, dove erano nella versione precedente del **Server**.
8. Se si utilizza il database esterno, ripristinare il database sul **Server** nuovo, indicare nel file di configurazione `drwcsd.conf` il percorso al database.

   Avviare dalla riga di comando il file `drwcsd.exe` con la

chiave `upgradedb` per aggiornare i database. La riga di comando completa avrà l'aspetto simile a:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" upgradedb "C:\Program Files
\DrWeb Enterprise Server\update-db"
```

9. Avviare **Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).

***All'aggiornamento di Dr.Web Enterprise Server della versione 4.XX alla versione 6.0.4 si consiglia di eseguire le seguenti azioni:***

1. Prima dell'aggiornamento disattivare i protocolli di **Installazione di rete** e di **Agent**. Per farlo, scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra che si apre scegliere la voce del menu di gestione **Configurazione di Dr.Web Enterprise Server,** passare alla scheda **Moduli**. Togliere i flag **Protocollo di Dr.Web Enterprise Agent** e **Protocollo di Dr.Web Network Installer** e premere **Salvare**.
2. Eseguire l'aggiornamento del **Server** alla versione **6.0.4** come descritto sopra (salvando il file di configurazione del **Server**).
3. Dopo l'aggiornamento del **Server** configurare l'elenco dei componenti installati sulle workstation (v. Contenuti pacchetto antivirus), in particolare, se non si dispone di licenza **Antispam**, impostare il valore **non può** per componenti **SpIDer Gate** e **Controllo Ufficio**.
4. Eseguire l'aggiornamento dei componenti di **Dr.Web ESS**. Per farlo, scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra che si apre scegliere la voce del menu di gestione **Stato repositorio**. Per verificare la disponibilità di aggiornamenti sul server **SAM**, premere il tasto **Verificare aggiornamenti**. Se necessario, prima definire le impostazioni dei server proxy per l'aggiornamento via **SAM**.
5. Se necessario, modificare le porte, che utilizzano gli **Agent** per comunicare con il **Server**. Per farlo, utilizzare il menu **Amministrazione** → **Configurazione di Dr.Web Enterprise Server** → scheda **Trasporto**.

6. Attivare i protocolli di **Installazione di rete** e di **Agent**, disattivati al passo **1**.
7. Aggiornare il software sulle workstation.



Dopo l'aggiornamento del **Server** della versione **4.XX** alla versione **6.0.4** è necessario che nel file di configurazione del **Server** `drwcsd.conf` sia impostato il parametro `Transport`:

```
Transport "drwcs" "tcp/0.0.0.0:2193" "udp/231.0.0.1:2193"
```

dove `drwcs` è il nome del **Server**.

Se tale parametro non è impostato, aggiungerlo manualmente e riavviare il **Server**.

## 9.1.2. Aggiornamento di Dr.Web Enterprise Server per i SO della famiglia UNIX®

Aggiornamento del software del **Server** con la versione installata è disponibile solo per alcuni SO della famiglia UNIX. Quindi nei SO della famiglia UNIX, dove non si può eseguire l'aggiornamento sopra il pacchetto già installato, si deve eliminare il software del **Server** delle versioni precedenti e installare il software della versione **6.0.4**.

### *Salvataggio dei file di configurazione*

All'eliminazione del **Server** i seguenti file vengono salvati automaticamente:

| File | Descrizione | Cartella predefinita |
|---|---|---|
| `dbinternal.dbs` | database interno | • per SO Linux: /var/opt/drwcs/<br>• per SO Solaris e FreeBSD: /var/drwcs/ |

| File | Descrizione | Cartella predefinita |
|---|---|---|
| drwcsd.conf (nome può essere diverso) | file di configurazione del **Server** | • per SO Linux: /var/opt/drwcs/etc<br>• per SO Solaris e FreeBSD: /var/drwcs/etc |
| webmin.conf | file di configurazione del **Centro gestione** | |
| common.conf | file di configurazione (per alcuni SO della famiglia UNIX) | |
| enterprise.key (nome può essere diverso) | chiave di licenza di **Server** | |
| agent.key (nome può essere diverso) | chiave di licenza di **Agent** | |
| certificate.pem | certificato per SSL | |
| private-key.pem | chiave chiusa RSA | |
| drwcsd.pri | chiave di codifica chiusa | |
| drwcsd.pub | chiave di codifica aperta | per SO Linux e SO Solaris:<br>• /opt/drwcs/Installer/<br>• /opt/drwcs/webmin/install<br>per SO FreeBSD:<br>• /usr/local/drwcs/Installer/<br>• /usr/local/drwcs/webmin/install |

## *Salvataggio della base di dati*

Prima di aggiornare il software **Dr.Web Enterprise Security Suite**, si raccomanda di eseguire copiatura di riserva della base di dati.

***Per salvare la base di dati:***

1. Arrestare il **Server**.
2. Esportare la base di dati nel file:
   - In caso di SO FreeBSD:
     ```
     # /usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/etc/esbase.es
     ```
   - In caso di SO Linux:
     ```
     # /etc/init.d/drwcsd exportdb /var/opt/drwcs/etc/esbase.es
     ```
   - In caso di SO Solaris:
     ```
     # /etc/init.d/drwcsd exportdb /var/drwcs/etc/esbase.es
     ```

In caso dei **Server** che utilizzano base di dati esterna, si raccomanda di utilizzare strumenti standard, forniti insieme alla base di dati.



Assicurarsi che l'esportazione della base di dati di **Dr.Web ESS** si sia completata con successo. L'assenza di una copia di riserva della base di dati non farà possibile ripristinare il **Server** in caso di emergenza.

## *Note importanti*



Tutte le azioni dell'aggiornamento sono da eseguire dal nome dell'amministratore **root**.

Se si aggiorna il **Server** fino alla versione **6.0.4** dalla versione **5.0** e inferiore, è necessario rimuovere completamente il repository e installare la sua versione nuova.

Se la rete antivirus ha una configurazione a più server, solo le basi di dati dei virus verranno trasmesse dal **Server** master dalla versione **6.0.4** ai **Server** slave dalla versione **5.0** e inferiore.

Per passare gli aggiornamenti di tutto il software antivirus, si deve aggiornare il **Server** slave fino alla versione **6.0.4** (per compatibilità di struttura dei repositori).

Partendo dalla versione **5.0**, nel pacchetto antivirus **Dr.Web Enterprise Security Suite** sono inclusi i prodotti **SpIDer Gate** e **Controllo Ufficio**, per poter utilizzare i quali devono essere indicati nella licenza (**Antivirus +Antispam**). Se tali prodotti non sono indicati nella licenza, si consiglia di eseguire le azioni, descritte sotto

## Aggiornamento automatico

All'aggiornamento del **Server** della versione **5.0** e superiori alla versione **6.0.4** per i SO **Linux**, invece di eliminare la versione precedente e installare una versione del **Server** nuova, si possono utilizzare i comandi seguenti per aggiornare il **Server**:

- per **rpm**: `rpm -U` *<nome pacchetto>*
- per **dpkg**: `dpkg -i` *<nome pacchetto>*

In questo caso tutti i file salvati automaticamente saranno locate nelle cartelle richieste e non si richiede la sostituzione manuale.

In caso di aggiornamento del pacchetto nelle distribuzioni **rpm** per **Server** dalle versioni **5.0** o **6.0**, se prima dell'aggiornamento di **Server**, sono state apportate modifiche nel file di configurazione di **Centro gestione** `webmin.conf`, il file `webmin.conf` viene salvato secondo la versione vecchia, e il nuovo file viene creato con il nome `webmin.conf.rpmnew`.

Se è necessario usare le funzionalità impostate dai parametri modificati del file di configurazione (compresa la possibilità che il programma di installazione di **Agent** sia accessibile all'indirizzo http://*<server_name>*:9080/install, v. File di installazione), trasferire tutte le impostazioni modificate dal file vecchio in quello nuovo e rinominare il file nuovo `webmin.conf.rpmnew` in `webmin.conf` sostituendo il file vecchio.

## Aggiornamento manuale

***Per aggiornare Dr.Web Enterprise Server se si utilizza il database interno:***

1. Arrestare il **Server**.
2. Se ci sono i file da utilizzare ulteriormente (a parte i file, che saranno salvati automaticamente all'eliminazione del **Server** al passo **4**), creare le copie di riserva di tali file manualmente, per esempio, i moduli di log ecc.
3. Eliminare tutti i contenuti del repositorio.
4. Eliminare il software del **Server** (v. Eliminazione di Dr.Web Enterprise Server per i SO della famiglia UNIX®). A questo si propone automaticamente di salvare le copie di riserva dei file. Per farlo è sufficiente inserire il percorso per salvarle o accettare il percorso predefinito.
5. Installare **Enterprise Server** della versione **6.0.4** secondo la procedura regolare di installazione (v. Installazione di Dr.Web Enterprise Server per i SO della famiglia UNIX®).
6. Se necessario, sostituire i file, creati all'installazione, con i file automaticamente salvati all'eliminazione del **Server** della versione precedente. I file da sostituire si trovano nelle seguenti cartelle:

| File | Percorso per SO | | |
|---|---|---|---|
| | Linux | Solaris | FreeBSD |
| drwcsd.pub | /opt/drwcs/Installer/<br>/opt/drwcs/webmin/install | | /usr/local/drwcs/Installer/<br>/usr/local/drwcs/webmin/install |
| dbinternal.dbs | /var/opt/drwcs/ | /var/drwcs/ | |
| drwcsd.conf<br>drwcsd.pri<br>enterprise.key<br>agent.key<br>certificate.pem<br>private-key.pem | /var/opt/drwcs/etc | /var/drwcs/etc | |



Il file di configurazione di **Centro gestione** (`webmin.conf`) dalle versioni inferiori a **6.0.2** non è compatibile al software dalla versione **6.0.4**. Se il **Server** viene reinstallato a partire da una versione inferiore a **6.0.2**, questo file non può essere sostituito con una copia salvata automaticamente. Tutte le impostazioni necessarie, memorizzate in questo file devono essere inserite a mano.

Se qualche file è stato salvato manualmente, è da locare nelle stesse cartelle, dove si è trovato nella versione precedente del **Server**.



Per tutti i file salvati dalla versione precedente di **Server** (v. passo **6**) è necessario impostare come titolare di file l'utente selezionato all'installazione della nuova versione di **Server** (di default - **drwcs**).

7. Eseguire i comandi:
   - per i SO **Linux** e i SO **Solaris**:
     ```
     /etc/init.d/drwcsd upgradedb
     ```
   - per i SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh upgradedb
```

8. Avviare il **Server**.
9. Configurare l'aggiornamento del repositorio e aggiornarlo completamente.
10. Riavviare il **Server**.

***Per aggiornare Dr.Web Enterprise Server se si utilizza il database esterno:***

1. Arrestare il **Server**.
2. Se ci sono i file da utilizzare ulteriormente (a parte i file, che saranno salvati automaticamente all'eliminazione del **Server** al passo **4**), creare le copie di riserva di tali file manualmente, per esempio, i moduli di log ecc.
3. Eliminare tutti i contenuti del repositorio.
4. Eliminare il software del **Server** (v. Eliminazione di Dr.Web Enterprise Server per i SO della famiglia UNIX®). A questo si propone automaticamente di salvare le copie di riserva dei file. Per farlo è sufficiente inserire il percorso per salvarle o accettare il percorso predefinito.
5. Installare **Enterprise Server** della versione **6.0.4** secondo la procedura regolare di installazione (v. Installazione di Dr.Web Enterprise Server per i SO della famiglia UNIX®).
6. Mettere i file salvati automaticamente (v. sopra):
   - per i SO **Linux**:

     nella cartella `/var/opt/drwcs/etc`, oltre chiave `pub`, che è da mettere nella `/opt/drwcs/Installer/` e nella `/opt/drwcs/webmin/install`
   - per i SO **FreeBSD**:

     nella cartella `/var/drwcs/etc`, oltre chiave `pub`, che è da mettere nella `/usr/local/drwcs/Installer/` e nella `/usr/local/drwcs/webmin/install`
   - per i SO **Solaris**:

     nella cartella `/var/drwcs/etc`, oltre chiave `pub`, che è da mettere nella `/opt/drwcs/Installer/` e nella `/opt/drwcs/webmin/install`

Se alcuni file sono stati salvati manualmente, metterli nelle stesse cartelle, dove si trovavano nella versione precedente del **Server**.



Per tutti i file salvati dalla versione precedente di **Server** (v. passo **6**) è necessario impostare come titolare di file l'utente selezionato all'installazione della nuova versione di **Server** (di default - **drwcs**).

7. Eseguire i comandi:
   - per i SO **Linux** e i SO **Solaris**:
     ```
     /etc/init.d/drwcsd upgradedb
     ```
   - per i SO **FreeBSD**:
     ```
     /usr/local/etc/rc.d/drwcsd.sh upgradedb
     ```
8. Avviare il **Server**.
9. Impostare l'aggiornamento del repositorio e aggiornarlo completamente.
10. Riavviare il **Server**.

***All'aggiornamento di Dr.Web Enterprise Server della versione 4.XX alla versione 6.0.4 si consiglia di eseguire le seguenti azioni:***

1. Prima del processo di aggiornamento disattivare i protocolli di **Installazione di rete** e di **Agent**. Per eseguirlo, scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, e nella finestra che si apre scegliere la voce del menu di gestione **Configurazione Enterprise Server,** quindi passare sulla scheda **Moduli**. Togliere i flag da **Protocollo Dr.Web Enterprise Agent** e da **Protocollo Dr.Web Network Installer** e cliccare **Salva**.
2. Eseguire l'aggiornamento del **Server** alla versione **6.0.4** come descritto sopra (salvando il file di configurazione del **Server**).
3. Dopo l'aggiornamento del **Server** impostare l'elenco dei componenti installati sulle workstation (v. Contenuti pacchetto antivirus), in particolare, se non si dispone di licenza **Antispam**, impostare il valore **non può** per componenti **SpIDer Gate** e **Controllo Ufficio**.

4. Eseguire l'aggiornamento dei componenti di **Dr.Web ESS**. Per farlo, scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra che si apre scegliere la voce del menu di gestione **Stato del repository**. Per verificare la disponibilità di aggiornamenti sul server **SAM**, premere il tasto **Verifica aggiornamenti**. Se necessario, definire prima le impostazioni dei server proxy per aggiornare tramite **SAM**.
5. Se necessario, modificare le porte, che utilizzano gli **Agent** per comunicare con il **Server**.
6. Attivare i protocolli di **Installazione di rete** e di **Agent**, disattivati al passo **1**.
7. Aggiornare il software sulle workstation.



Dopo l'aggiornamento del **Server** della versione **4.XX** fino alla versione **6.0.4** è necessario che nel file di configurazione del **Server** `drwcsd.conf` sia impostato il parametro `Transport`:

```
Transport "drwcs" "tcp/0.0.0.0:2193" "udp/231.0.0.1:2193"
```

dove `drwcs` è il nome del **Server**.

Se tale parametro non è impostato, aggiungerlo manualmente e riavviare il **Server**.

## 9.1.3. Aggiornamento di plug-in Dr.Web Browser-Plugin

Per aggiornare il plug-in **Dr.Web Browser-Plugin** (viene utilizzato dal **Centro gestione**) si deve eliminare manualmente la versione precedente del plug-in ed installare un plug-in nuovo **Dr.Web Browser-Plugin**.

Eliminazione del plug-in è descritta in Eliminazione dei componenti software per i SO Windows® e in Eliminazione di Dr.Web Enterprise Server per i SO della famiglia UNIX®.

Il processo di installazione è descritto in Installazione di plug-in Dr.Web Browser-Plugin.

### 9.1.4. Aggiornamento di Dr.Web Enterprise Agent

Dopo l'aggiornamento del software del **Server** tutti gli **Agent**, collegati ad esso, vengono aggiornati automaticamente.



I consigli su aggiornamento di **Agent**, installati su workstation, che eseguono le funzioni importanti di LAN, sono riportati nella sezione Aggiornamento di Agent su server LAN.

### 9.1.5. Aggiornamento di Proxy

#### Aggiornamento del Proxy per SO Windows

L'aggiornamento automatico del **Proxy** non si supporta.

All'avvio di programma di installazione su un computer su cui è installato il **Proxy**:

- Se si avvia un programma di installazione che ha lo stesso numero di bit che il **Proxy** installato, viene visualizzato un avviso dell'impossibilità dell'installazione.
- Se si avvia un programma di installazione che ha un numero di bit diverso da quello del **Proxy** installato, il **Proxy** verrà installato in una cartella diversa dalla cartella della versione già installata.



Se sullo stesso computer vengono installati due **Proxy** che utilizzano per il loro funzionamento la stessa porta, questo comporta inoperatività di entrambi **Proxy**.

***Per aggiornare il Proxy:***

1. Se sul computer, su cui è installato **Proxy,** è installato **Agent** con auto-difesa attivata, disabilitare il componente di auto-difesa **Dr.Web SelfPROtect** nelle impostazioni di **Agent**.
2. Eliminare il **Proxy** secondo la procedura standard (vedi la voce Eliminazione del Proxy).



All'eliminazione del **Proxy** si elimina il file di configurazione `drwcsd-proxy.xml`. Se necessario, salvare il file di configurazione manualmente prima dell'eliminazione del **Proxy**.

3. Installare la nuova versione di **Proxy** secondo la procedura standard (vedi Installazione di Server Proxy).
4. Se necessario, sostituire il file di configurazione con quello salvato nella versione precedente.
5. Se al passo 1 è stato disabilitato il componente di auto-difesa **Dr.Web SelfPROtect**, abilitare questo componente nelle impostazioni di **Agent**.

## Aggiornamento del Proxy per SO della famiglia UNIX

***Per aggiornare il Proxy eseguire:***

| Per il Proxy in | | Comando |
|---|---|---|
| SO FreeBSD<br>SO Solaris | | Eseguire eliminazione e installazione nuova secondo le procedure standard descritte nelle sezioni Eliminazione di Proxy e Installazione di Proxy |
| SO Linux | pacchetto deb | `dpkg -i drweb-esuite-proxy` |

| Per il Proxy in | | Comando |
|---|---|---|
| | pacchetto rpm | `rpm -U drweb-esuite-proxy` |
| | pacchetto generic | Spacchettare il pacchetto di installazione tramite il seguente comando:<br>`tar -xjf <nome_file_distribuzione>.tar.bz2`<br>Dopo questo sostituire manualmente i file della cartella di installazione del **Proxy** con i file dall'archivio spacchettato. |

# 9.2. Aggiornamento manuale dei componenti di Dr.Web Enterprise Security Suite



Prima di aggiornare **Dr.Web ESS** e i componenti singoli di esso si consiglia di controllare la correttezza delle impostazioni del protocollo TCP/IP per poter accedere ad Internet. In particolare, il servizio DNS deve essere attivo e avere le impostazioni corrette.

## Verifica della disponibilità di aggiornamenti

***Per verificare la disponibilità di aggiornamenti dei prodotti di Dr.Web ESS sul server di aggiornamenti:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Stato del repository**.
2. Nella finestra aperta viene visualizzata l'informazione su tutti i componenti, nonché la data di ultima revisione di essi e lo stato attuale. Per verificare la disponibilità di aggiornamenti sul server **SAM**, premere il tasto **Verifica aggiornamenti.**
3. Se il componente verificato è obsoleto, il suo aggiornamento

avviene automaticamente nel processo della verifica. L'aggiornamento viene eseguito secondo le impostazioni del repositorio (v. voce Gestione repositorio di Dr.Web Enterprise Server).

4. Dopo il completamento di aggiornamento, i componenti aggiornati nella riga **L'ultima revisione del** avranno la data attuale.

## Avvio del processo di aggiornamento del software della workstation

***Per avviare il processo di aggiornamento del software della workstation:***

1. Scegliere la voce **Rete antivirus** del menu principale del **Centro gestione**, nella finestra aperta nella lista gerarchica cliccare sul nome di workstation o di gruppo.
2. Nella barra degli strumenti premere il tasto **Gestione dei componenti**. Nel sottomenu aperto scegliere la voce:
   - **Aggiornare componenti falliti**, se si vogliono aggiornare solamente i componenti, il cui aggiornamento precedente è andato in errore, e corregere lo stato dell'errore,
   - **Aggiornare tutti i componenti**, se si vuole avviare l'aggiornamento forzato di tutti i componenti, compresi quelli con l'ultima versione già installata.



Durante l'aggiornamento forzato di tutti i componenti sono necessari due riavvii della workstation. Seguire le istruzioni di **Agent**.

Si può eseguire questa operazione con gli strumenti di gestione di **Enterprise Agent** stesso.

***Per avviare il processo di aggiornamento del software della workstation con Dr.Web Enterprise Agent***

1. Consentire all'utente di questa workstation introdurre le modifiche nelle impostazioni di **Enterprise Agent** (v. Configurazione diritti utenti).
2. Scegliere nel menu contestuale dell'icona dell'**Agent** la voce **Sincronizzare**.
3. Nel sottomenu aperto scegliere la voce:
   - **Solo i componenti guasti**, se si vogliono aggiornare solamente i componenti, il cui aggiornamento precedente è andato in errore, e corregere lo stato dell'errore,
   - **Tutti i componenti**, se si vuole avviare l'aggiornamento dei componenti guasti, come descritto sopra, e di tutti gli altri componenti.

## Errore critico dell'aggiornamento

***Nel caso di errore critico dell'aggiornamento:***

1. Avviare il processo di aggiornamento completo forzato della workstation (v. sopra).
2. Se l'errore non è risolto, trovare la causa dell'errore con i file del protocollo di **Agent** e di modulo di aggiornamento della workstation (di default essi sono locati nella sottocartella `logs` della cartella di installazione dell'**Agent**, file `drwagntd.log` e `drwupgrade.log` rispettivamente).
3. Eliminare la causa dell'errore e avviare di nuovo il processo dell'aggiornamento forzato della workstation.

# 9.3. Aggiornamento programmato

Si può impostare l'orario di esecuzione dei processi sul **Server** per eseguire aggiornamenti regolari del software (per più informazioni sul programmi dei processi v. Configurazione dell'orario di Dr.Web Enterprise Server).

***Per configurare l'orario dell'esecuzione del processo all'aggiornamento sul server Dr.Web Enterprise Server:***

1. Scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Orario Dr.Web Enterprise Server**. Si apre la lista corrente dei processi del **Server**.
2. Per aggiungere un processo alla lista, premere nella barra degli strumenti il tasto  **Nuovo task**. Si apre la finestra di modifica del processo.
3. Inserire nel campo **Nome** il nome del processo, con il quale sarà visualizzato nell'orario.
4. Passare alla scheda **Azione** e scegliere nella lista a cascata il tipo di processo **Aggiornamento**.
5. Nella lista a cascata apparsa scegliere il componente aggiornato dal processo:
   - **Dr.Web Enterprise Agent**
     **Dr.Web Enterprise Server**
     **Dr.Web Enterprise Updater**
     **Dr.Web per UNIX**
     **Dr.Web Virus Bases**
   - **Tutti i prodotti di Dr.Web Enterprise**, se si vuole impostare il processo di aggiornamento di tutti i componenti di **Dr.Web ESS**.



Per le versioni **5.0** e superiori gli aggiornamenti del software del **Server** non vengono forniti dai server **SAM**.

Per l'aggiornamento del **Server** utilizzare la versione richiesta del programma di installazione ed eseguire l'aggiornamento secondo le regoli generali, riportate nelle sezioni Aggiornamento di Dr.Web ESS per i SO Windows® o Aggiornamento di Dr.Web ESS per i SO della famiglia UNIX®.

6. Passare alla scheda **Tempo** e indicare nella lista a cascata la periodicità dell'avvio del processo, dopodiché impostare l'ora secondo la periodicità scelta (questa azione è simile all'impostazione dell'ora nell'orario della workstation, v. Configurazione orario di processi su workstation).

7. Per salvare le modifiche, premere il tasto **Salva**.

# 9.4. Aggiornamento repositorio Dr.Web Enterprise Server, non connesso a Internet

Se **Enterprise Server** non è connesso a Internet, si può aggiornare il suo repositorio manualmente, copiando il repositorio di altro **Enterprise Server** aggiornato.



Questo metodo non è adatto per passare a un'altra versione.

Per la versione **5.0** e superiori gli aggiornamenti del software del **Server** stesso dai server **SAM** non vengono forniti.

Per aggiornare il **Server** stesso, utilizzare l'installazione della versione richiesta ed eseguire la procedura di aggiornamento secondo le regole comuni, riportate nelle sezioni Aggiornamento di Dr.Web ESS per i SO Windows® o Aggiornamento di Dr.Web ESS per i SO della famiglia UNIX®.

***Per ottenere aggiornamenti del software antivirus si consiglia di eseguire le seguenti operazioni:***

1. Installare il software di **Enterprise Server** sul computer, che ha accesso a Internet, come descritto in Installazione di server antivirus.
2. Sospendere tutti e due **Enterprise Server**.
3. Per ottenere aggiornamenti del software antivirus avviare il **Server**, connesso a Internet, con la chiave `syncrepository`.

   Esempio per il SO **Windows**:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin
   ```

```
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" syncrepository
```

4. Completamente sostituire i contenuti della cartella di repositorio del **Server** principale (operativo) con i contenuti della cartella analoga del repositorio del **Server**, connesso ad Internet. Di solito è:
   - `var\repository` nel SO **Windows**,
   - `/var/drwcs/repository` nei SO **FreeBSD** e SO **Solaris**,
   - `/var/opt/drwcs/repository` nel SO **Linux**.



Se sul computer con **Enterprise Server** è installato un **Agent** con il componente di autoprotezione **Dr.Web SelfPROtect** attivato, prima di aggiornare il repositorio si deve disattivare tale componente via impostazioni di **Agent**.

5. Se il **Server** principale opera nei SO della famiglia UNIX, su repositorio copiato si devono installare i diritti di utente, creato/scelto durante l'installazione di questo **Server**.
6. Eseguire sul **Server** principale il comando:

```
drwcsd rerepository
```

Nel SO **Windows** il comando può essere avviato sia dalla *riga di comando*:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" rerepository
```

sia dal menu `Start` → `Programmi` → `DrWeb Enterprise Server` → `Gestione server` → `Riavviare il repositorio`.

7. Avviare il **Server** principale.



Se durante l'aggiornamento del repositorio è stato disattivato il componente di autoprotezione di **Dr.Web SelfPROtect**, si consiglia di ripristinare il funzionamento di tale componente.

# 9.5. Limitazione di aggiornamenti di workstation

Con **Centro gestione** si può impostare la modalità di aggiornamenti (consentiti/bloccati) per i componenti di **Dr.Web Enterprise Security Suite** su workstation protette in certi orari. Per farlo:

1. Scegliere la voce **Rete antivirus** del menu principale, nella finestra aperta nell'elenco gerarchico cliccare sul nome della workstation o nome del gruppo. Nel menu di gestione (pannello a sinistra) scegliere la voce **Limitazione degli aggiornamenti**.
2. Si apre la tabella, dove si imposta la modalità di aggiornamento nella seguente gradazione a colori:
   - colore verde - aggiornamento consentito;
   - colore rosso - aggiornamento proibito.

   La limitazione viene impostata per ogni 15 minuti di ogni giorno della settimana.




3. Per modificare la modalità di aggiornamenti cliccare sul blocco corrispondente della tabella.

   Per modificare la modalità della riga intera (un giorno completo), cliccare sull'evidenziatore del colore corrispondente a

destra della riga richiesta della tabella.

Per modificare la modalità della colonna intera (ogni intervallo di 15 minuti per tutti i giorni della settimana), cliccare sull'evidenziatore del colore corrispondente sotto la colonna richiesta della tabella.

4. Finite le modifiche, premere il tasto **Salva** per accettare le modifiche apportate.

Nella barra degli strumenti sono disponibili le seguenti opzioni:

**Propaga queste impostazioni verso un altro oggetto** - per copiare le impostazioni di aggiornamento della workstation o del gruppo nelle impostazioni di altro workstation o di altro gruppo.

**Ripristinare le impostazioni** - per ripristinare le impostazioni ai valori predefiniti (tutti gli aggiornamenti sono consentiti).

**Esporta le impostazioni nel file** - per salvare le impostazioni di aggiornamento nel file del formato speciale.

**Importa le impostazioni dal file** - per caricare le impostazioni di aggiornamento dal file del formato speciale.

## 9.6. Aggiornamento di Agent mobili Dr.Web Enterprise Agent

Se computer (o portatile) per un lungo periodo di tempo non avrà connessione a **Enterprise Server**, per ottenere tempestivamente gli aggiornamenti dai server di **SAM** di **Dr.Web** si consiglia di impostare la modalità mobile dell'operazione di **Enterprise Agent**. Per farlo, nel menu contestuale di icona di **Agent** nell'area di notifica di **Barra delle applicazioni** scegliere **Modalità mobile → Consentita**. Il colore di icona di **Agent** diventerà giallo.

Nella modalità mobile **Agent** cerca di connettersi al **Server**, ne fa tre tentativi, e, se non ci è riuscito, esegue HTTP-aggiornamento. I tre tentativi di trovare il **Server** sono vengono fatti in maniera continua

con un intervallo di circa un minuto.



Variante **Modalità mobile** sarà disponibile nel menu contestuale solo se nei diritti di workstation è consentita la modalità mobile di utilizzo di **SAM** di **Dr.Web** (per più informazioni v. Configurazione dirirtti utenti).



Durante il funzionamento di **Agent** nella modalità mobile la connessione di **Agent** a **Enterprise Server** interrompe. Tutte le modifiche, che si impostano nel **Server** per tale workstation, entrano in vigore non appena la modalità mobile dell'operazione di **Agent** viene disattivata, e la connessione di **Agent** al **Server** viene ripristinata.

Nella modalità mobile si esegue solamente l'aggiornamento dei database dei virus.

Per configurare le impostazioni della modalità di operazione mobile scegliere **Modalità mobile** → **Impostazioni**. Nel campo **Periodicità** indicare la frequenza con quale verificare la disponibilità di aggiornamenti in **SAM**. Se necessario, mettere il flag **Solo a connessione a Internet**.

Se si utilizza il server proxy, nel campo **Proxy** mettere il flag su **Utilizzare server proxy** e sotto nei campi di input indicare l'indirizzo e la porta del server proxy, nonché i parametri di autorizzazione.

Per avviare immediatamente l'aggiornamento nella modalità mobile, scegliere **Modalità mobile** → **Avviare aggiornamento**.



Voce **Avviare aggiornamento** non sarà disponibile, se c'è la connessione al **Server**.

Per disattivare la modalità mobile, nel menu contestuale di icona di **Agent** scegliere **Modalità mobile** e togliere il flag da **Consentita**. Il colore di icona di **Agent** da giallo diventerà verde e la connessione di **Agent** al **Server** verrà ripristinata.

# 9.7. Aggiornamento di chiave di server e di chiave di workstation

I file contenenti la chiave di server e la chiave di workstation vengono installati insieme a **Enterprise Server** (v. Installazione di Dr.Web Enterprise Server). Di seguito si possono ottenere le chiavi nuove, per esempio, con il periodo di validità di licenza più lungo.

Ci sono due varianti della procedura di sostituzione dei file della chiave, secondo se corrispondono i parametri di **Server** `ID` del file della chiave nuovo e di quello precedente. Aprire la chiave nuova e quella precedente `enterprise.key` con qualsiasi editor di testo e nella sezione `[Enterprise]` verificare il valore del parametro `ID1`.



Il file della chiave è nel formato, protetto dalla modifica con il meccanismo di firma elettronica. La modifica del file lo rende non valido. Per evitare il guasto accidentale del file della chiave, non si deve modificarlo e/o salvarlo alla chiusura di editor di testo.

Se sul computer con **Enterprise Server** è installato **Agent** con il componente di auto-protezione **Dr.Web SelfPROtect** attivato, prima di sostituire i file della chiave è necessario disattivare tale componente via le impostazioni di **Agent**.

## I valori dei parametri ID1 corrispondono



Per installare i file della chiave nuovi dei componenti della rete antivirus utilizzare il Gestore licenze.

***Per installare i file della chiave nuovi dei componenti della rete antivirus manualmente:***

1. Mettere il file della chiave di server (deve avere il nome `enterprise.key`) nella sottocartella `etc` della cartella di installazione del **Server** per sostituire il file che è presente lì con lo stesso nome.
2. Riavviare il **Server**.
3. Nella cartella della rete antivirus scegliere il gruppo **Everyone**, dopodiché nella barra degli strumenti cliccare **Generali** → **Importo della chiave**.
4. Nella finestra aperta indicare il file della chiave di workstation (`agent.key`) e cliccare **OK**.

## I valori dei parametri ID1 sono diversi

***Per installare i file della chiave nuovi dei componenti della rete antivirus:***

1. Distattivare i protocolli di **Agent** e di **Installazione di rete.** Per farlo, scegliere la voce **Amministrazione** del menu principale di **Centro gestione**, nella finestra che si apre scegliere la voce del menu di gestione **Configurazione Dr.Web Enterprise Server**, passare alla scheda **Moduli**. Togliere i flag da **Protocollo Dr.Web Enterprise Agent** e da **Protocollo Dr.Web Network Installer** e cliccare **Salva**. Si richiederà il riavvio del **Server**. Cliccare **Sì**.
2. Esportare l'orario di **Enterprise Server** nel file. Per farlo, scegliere la voce **Amministrazione** del menu principale di **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Orario Dr.Web Enterprise Server** e nella barra degli strumenti cliccare **Esporta le impostazioni nel file**.
3. Per risparmiare lo spazio nel database eliminare l'orario di **Enterprise Server**. Per farlo, scegliere la voce **Amministrazione** del menu principale di **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Orario di Dr.Web Enterprise Server** e nella barra degli

strumenti cliccare  **Rimuovi queste impostazioni**.

4. Nel caso della rete a più server:
   a) Se è necessario salvare informazioni statistiche dei **Server** adiacenti, esportare tabelle delle statistiche, perché dopo l'eliminazione dei legami queste informazioni verranno perse.
   b) Eliminare tutte le relazioni impostate tra i server. Si può farlo tramite il menu **Amministrazione**, la voce **Relazioni**.
5. Installare i file della chiave nuovi dei componenti della rete antivirus:
   - Per farlo, utilizzare il Gestore licenze.
   - Per sostituire le chiavi manualmente utilizzare la procedura, descritta sopra.
6. Attivare i protocolli di **Agent** e di **Installazione di rete**, distattivati nella voce **1**.
7. Impostare l'orario del **Server** di nuovo o importare dal file l'orario precedente, salvato nella voce **2**.
8. Se nella rete ci sono più server, impostare tutte le comunicazioni dei server, eliminate nella voce **4**.
9. Riavviare il **Server**.

# Capitolo 10. Configurazione dei componenti supplementari

## 10.1. Server proxy

La rete antivirus può avere uno o più **Server proxy**.

Il compito principale del **Server proxy** è il mantenimento della comunicazione di **Enterprise Server** e di **Enterprise Agent** se non è possibile organizzare l'accesso diretto (per esempio, se **Enterprise Server** e **Enterprise Agent** sono locati nelle reti diverse, tra le quali non c'è il routing dei pacchetti).

### Funzionalità principali

***Server proxy esegue le seguenti funzioni:***

1. Ascolto della rete e accettazione di connessioni secondo il protocollo e la porta impostati.
2. Traslazione dei protocolli (sono supportati i protocolli TCP/IP, IPv6, IPX e NetBIOS).
3. Comunicazione dei dati tra **Enterprise Server** e **Enterprise Agent** secondo le impostazioni del server proxy.
4. Caching di aggiornamenti di **Agent** e del pacchetto antivirus, trasmessi dal **Server**. Se gli aggiornamenti vengono forniti dal cache del **Server proxy**:
   - diminuisce il traffico di rete,
   - diminuisce il tempo di ricevimento aggiornamenti da **Agent**.



Si può creare gerarchia dei **Server proxy**.

Lo schema generale della rete antivirus con utilizzo del **Server proxy** è riportato nell'immagine 10-1.

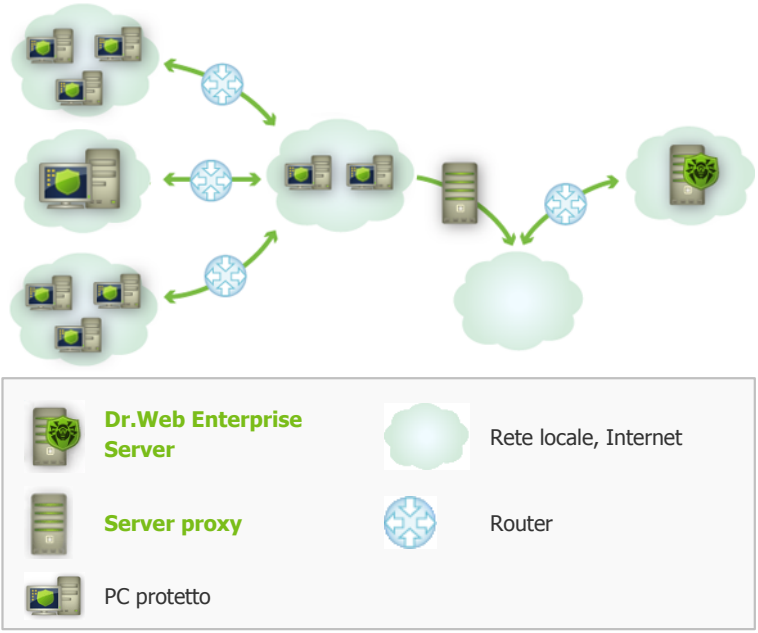



**Immagine 10-1. Schema della rete antivirus con utilizzo del Server proxy**

## Principio del funzionamento

***Se si utilizza il server proxy, viene eseguita la seguente serie di azioni:***

1. Se nell'**Agent** non è definito l'indirizzo del **Server**, l'**Agent** spedisce la richiesta a più indirizzi secondo il protocollo di rete, dove è situato.
2. Se il **Server proxy** è configurato alla traslazione delle connessioni (parametro `discovery="yes"`), all'**Agent** viene spedito l'avviso della presenza di un **Server proxy** funzionante.

3. **Agent** imposta i parametri ottenuti del **Server proxy** come parametri di **Enterprise Server**. La comunicazione successiva viene fatta nel modo trasparente per l'**Agent**.
4. Secondo i parametri del file di configurazione il **Server proxy** ascolta le porte impostate per le connessioni in entrata con protocolli impostati.
5. Per ogni connessione in entrata da **Agent** il **Proxy** stabilisce la connessione a **Enterprise Server**

***Algoritmo di reindirizzamento se è disponibile una lista dei Enterprise Server:***

1. Il **Server proxy** carica nella memoria operativa una lista dei **Enterprise Server** dal file di configurazione `drwcsd-proxy.xml` (vedi Allegato G4).
2. Il **Enterprise Agent** si connette al **Server proxy**.
3. Il **Server proxy** reindirizza il **Enterprise Agent** al primo **Enterprise Server** dalla lista che si trova nella memoria operativa.
4. Il **Server proxy** ruota la lista caricata nella memoria operativa e sposta il **Enterprise Server** dalla prima voce alla fine della lista.



Il **Server proxy** non memorizza la sequenza modificata dei **Server** nel suo file di configurazione. Al riavvio del **Server proxy**, la lista dei **Enterprise Server** viene caricata nella memoria operativa nella sua versione originale, conservata nel file di configurazione.

5. Quando un altro **Agent** si connette al **Server proxy**, la procedura si ripete dal punto 2.
6. Se il **Enterprise Server** si disconnette dalla rete antivirus (per esempio, in caso di spegnimento o negazione del servizio), l'**Agent** si connette di nuovo al **Server proxy** e la procedura si ripete dal punto 2.



Scanner di rete, avviato sulla workstation della rete esterna per gli **Agent**, non può rilevare **Agent** installati.



Se il flag **Sostituire i nomi NetBios** è attivo e nella rete antivirus viene utilizzato **Server proxy**, per tutte le workstation, connesse al **Server** via il **Server proxy**, nel **Centro gestione** come nomi di workstation viene visualizzato il nome del computer, su cui è installato il **Server proxy**.

### *Codifica e compressione del traffico*

**Server proxy** supporta la compressione del traffico. Elaborazione dell'informazione trasmessa viene eseguita nonostante il fatto se il traffico è compresso o meno.

**Server proxy** non supporta la codifica del traffico. Esso analizza l'informazione trasmessa e, se il traffico tra **Enterprise Server** e **Agent** è codificato, il **Server proxy** passa alla modalità trasparente, cioè trasmette tutto il traffico tra **Server** e **Agent** senza alcuna analisi dei dati.



Se la modalità di codifica del traffico tra **Agent** e **Server** è abilitata, sul **Server proxy** non c'è il caching di aggiornamenti.

### *Caching*

**Server proxy** supporta il caching del traffico.

Il caching dei prodotti viene eseguito secondo le revisioni. Ogni revisione viene conservata in una cartella separata. Nella cartella per ogni revisione successiva sono riportati dei link rigidi (*hard links*) ai file esistenti delle revisioni precedenti e versioni originali dei file modificati. In questo modo, i file di ogni versione vengono conservati sul disco rigido in una copia unica, in tutte le cartelle delle revisioni successive sono riportati solamente i link ai file non modificati.

Eliminazione delle revisioni obsolete viene eseguita ogni ora. Vengono conservate solamente 3 ultime revisioni. Tutte le altre, essendo revisioni precedenti, sono considerate obsolete e vengono eliminate.

Inoltre, ogni 10 minuti vengono scaricati i file *memory mapped* non usati.

## Impostazioni

Il **Server proxy** non ha interfaccia grafica. La configurazione delle impostazioni viene eseguita via file di configurazione. Il formato del file di configurazione del **Server proxy** è riportato in Allegato G4.



La gestione delle impostazioni (modifica del file di configurazione) del **Server proxy** può essere eseguita solo dall'utente con i diritti dell'amministratore di tale computer.

Affinché **Server proxy** funzioni in modo corretto sotto i SO della famiglia Linux, dopo il riavvio del computer è necessario eseguire una configurazione di sistema della rete non utilizzando un Gestore reti.

## Avvio e arresto

Nel SO Windows l'avvio e l'arresto del **Server proxy** viene eseguito da strumenti standard via **Pannello di controllo** → **Strumenti di amministrazione** → **Servizi** → nella lista dei servizi fare il doppio click su **drwcsd-proxy** e nella finestra aperta scegliere l'azione necessaria.

Per i SO della famiglia UNIX l'avvio e l'arresto del **Server proxy** viene eseguito da comandi `start` e `stop` applicati agli script, creati nel processo di installazione di **Server proxy** (v. Installazione di un server proxy).

Inoltre per avviare il **Server proxy** nei SO Windows e nei SO della famiglia UNIX si può avviare il file eseguibile `drwcsd-proxy` con i parametri corrispondenti (v. Allegato H10. Server proxy).

# 10.2. NAP Validator

## Dati generali

*Microsoft® Network Access Protection (NAP)* rappresenta una piattaforma di policy, incorporata nei sistemi operativi Windows, che provvede alla maggiore sicurezza di rete. La sicurezza raggiunta è dovuta all'adempimento dei requisiti, richiesti dall'operabilità dei sistemi della rete.

Utilizzando la tecnologia NAP, si possono creare le policy personalizzate di operabilità per valutare lo stato del computer. Le valutazioni ottenuti vengono analizzati nei seguenti casi:

- prima di concedere accesso o interazione,
- per aggiornamento automatico dei computer che corrispondono ai requisiti per provvedere alla loro compatibilità continua,
- per portare alla conformità i computer che non corrispondono ai requisiti, nel modo tale che soddisfino i requisiti impostati.

Descrizione completa della tecnologia NAP è disponibile al http://www.microsoft.com/windowsserver2008/en/us/nap-product-home.aspx.

## Utilizzo di NAP in Dr.Web Enterprise Security Suite

**Dr.Web ESS** permette di utilizzare la tecnologia NAP per il controllo di operabilità del software anti-virus delle workstation protette. Il componente utilizzato per questo è **Dr.Web NAP Validator**.

***Al controllo di operabilità vengono utilizzati i seguenti strumenti:***

- Server NAP di controllo di operabilità installato e configurato.

- **Dr.Web NAP Validator** rappresenta un mezzo di valutazione di operabilità del software antivirus del sistema protetto (System Health Validator - SHV) per conto delle policy personalizzate di **Dr.Web**. Viene installato sul computer con server NAP.
- Agent di operabilità del sistema (System Health Agent - SHA). Viene installato automaticamente insieme al software di **Enterprise Agent** su workstation.
- **Enterprise Server** viene utilizzato come server di patch, che provvede alla operabilità del software antivirus delle workstation.

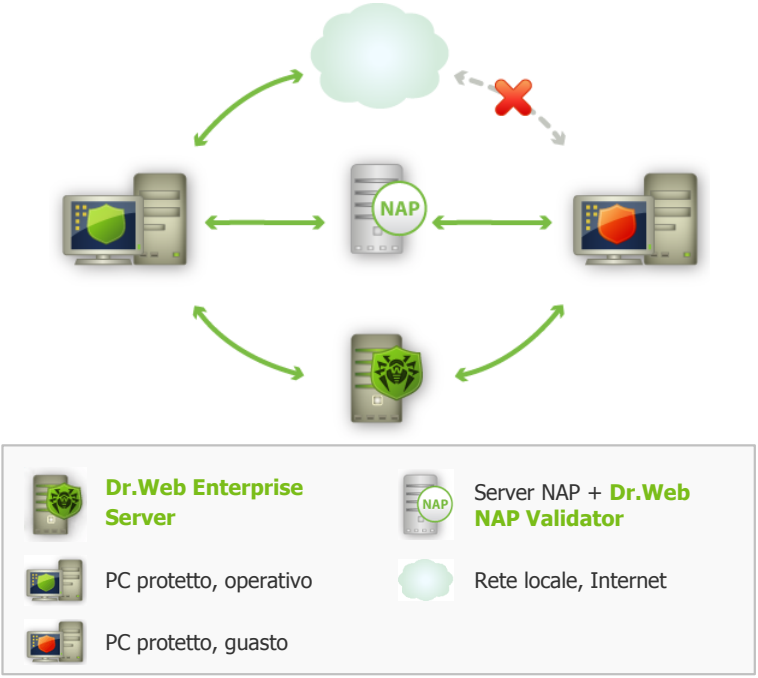



**Immagine 10-2. Schema della rete antivirus con l'utilizzo di NAP**

***Procedura di controllo viene eseguita nel modo seguente:***

1. Attivazione del processo di controllo viene eseguita alla configurazione delle impostazioni corrispondenti di **Agent** (v. Configurazione di Dr.Web Enterprise Agent).
2. SHA sulla workstation è connessa al componente **Dr.Web NAP**

**Validator**, installato sul server NAP.

3. **Dr.Web NAP Validator** esegue il controllo delle policy di operabilità (v. sotto). Il controllo delle policy rappresenta il processo, quando **NAP Validator** esegue valutazione dei mezzi antivirus dal punto di vista della conformità di essi alle regole impostate e definisce la categoria dello stato attuale del sistema:
   - workstation, che hanno passato il controllo di conformità agli elementi di policy, si ritengono operativi e sono ammessi all'operazione nella rete a piena funzionalità.
   - workstation, che non soddisfano almeno un parametro del policy, si ritengono non operativi. Tali workstation possono accedere solo a **Enterprise Server**, vengono isolati dal resto della rete. L'operabilità della workstation viene ripristinata con **Server**, dopodiché la workstation è soggetta di nuovo alla procedura di controllo.

***Requisiti all'operabilità:***

1. Stato funzionante dell'agent (avviato ed operativo).
2. Database dei virus aggiornati (database corrispondono ai database sul server).

## Configurazione di NAP Validator

Dopo l'installazione di **Dr.Web NAP Validator** (v. Installazione di NAP Validator) sul computer con il server NAP installato, sono da eseguire le seguenti azioni:

1. Aprire il componente della configurazione del server NAP (comando `nps.msc`).
2. Nella sezione **Policies** scegliere la sottovoce **Health Policies**.
3. Nella finestra aperta scegliere le proprietà dei componenti:

- **NAP DHCP Compliant**. Nella finestra delle impostazioni mettere il flag **Dr.Web System Health Validator**, che imposta utilizzo delle policy del componente **Dr.Web NAP Validator**. Nella lista a cascata dei tipi di controlli scegliere la voce **Client passed all SHV checks**. Secondo questa opzione, la workstation viene dichiarata operativa, se corrisponde a tutti gli elementi della policy impostata.
- **NAP DHCP Noncompliant**. Nella finestra delle impostazioni mettere il flag **Dr.Web System Health Validator**, che imposta utilizzo delle policy del componente **Dr.Web NAP Validator**. Nelle lista a cascata dei tipi di controlli scegliere la voce **Client fail one or more SHV checks**. Secondo questa opzione della workstation, essa viene dichiarata guasta, se non corrisponde almeno a uno di elementi della policy impostata.

# Allegati

## Allegato A. Lista completa delle versioni supportate dei SO

### Per Dr.Web Enterprise Server:

#### *SO della famiglia UNIX:*

ALT Linux School Server 5.0
ALT Linux School Server 5.0 x86_64
ASP Linux 12
ASP Linux 14
Debian/GNU Linux Lenny
Debian/GNU Linux Lenny x86_64
Debian/GNU Linux Sid x86_64
Debian/GNU Linux Squeeze
Debian/GNU Linux Squeeze x86_64
FreeBSD 7.3
FreeBSD 7.3 amd64
FreeBSD 7.4
FreeBSD 7.4 amd64
FreeBSD 8.1
FreeBSD 8.1 amd64
FreeBSD 8.2
FreeBSD 8.2 amd64
Linux glibc2.7
Linux glibc2.7 x86_64
Linux glibc2.8
Linux glibc2.8 x86_64

Linux glibc2.9
Linux glibc2.9 x86_64
Linux glibc2.10
Linux glibc2.10 x86_64
Linux glibc2.11
Linux glibc2.11 x86_64
Linux glibc2.12
Linux glibc2.12 x86_64
Linux glibc2.13
Linux glibc2.13 x86_64
Mandriva Linux 2010
Mandriva Linux 2010 x86_64
Mandriva Linux Corporate Server 5.1
Mandriva Linux Corporate Server 5.1 x86_64
openSUSE 11
openSUSE 11 x86_64
RedHat Enterprise Linux 5.3
RedHat Enterprise Linux 5.3 x86_64
RedHat Enterprise Linux 6
RedHat Enterprise Linux 6 x86_64
RedHat Fedora 8
RedHat Fedora 8 x86_64
RedHat Fedora 9
RedHat Fedora 9 x86_64
RedHat Fedora 10
RedHat Fedora 10 x86_64
RedHat Fedora 11
RedHat Fedora 11 x86_64
RedHat Fedora 12
RedHat Fedora 12 x86_64
RedHat Fedora 13
RedHat Fedora 13 x86_64
RedHat Fedora 14

RedHat Fedora 14 x86_64

RedHat Fedora 15

RedHat Fedora 15 x86_64

SUSE Linux Enterprise Server 10

SUSE Linux Enterprise Server 10 x86_64

SUSE Linux Enterprise Server 11

SUSE Linux Enterprise Server 11 x86_64

Sun Solaris 10 x86

Sun Solaris 10 Sparc 32bit (processore Sparc V9; UltraSparc come minimo)

Sun Solaris 10 Sparc 64bit (processore Sparc V9; UltraSparc come minimo)

Ubuntu 8.04

Ubuntu 8.04 x86_64

Ubuntu 10.04

Ubuntu 10.04 x86_64

Ubuntu 10.10

Ubuntu 10.10 x86_64

Ubuntu 11.04

Ubuntu 11.04 x86_64

Ubuntu 11.10

Ubuntu 11.10 x86_64

## *SO Windows:*

*- 32 bit:*

Windows 2000 Professional (SP4)

Windows 2000 Server (SP4)

Windows XP Professional (SP3)

Windows XP Home (SP3)

Windows Server 2003 (SP2)

Windows Vista (anche con SP1 e superiori)

Windows Server 2008 (anche con SP1 e superiori)

Windows 7
Windows 8

*- 64 bit:*

Windows Server 2003 (SP2)
Windows Vista (anche con SP1 e superiori)
Windows Server 2008 (anche con SP1 e superiori)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

## Per Dr.Web Enterprise Agent e pacchetto antivirus:

### *SO della famiglia UNIX:*

Linux glibc 2.7 e superiori
FreeBSD 7.3 e superiori
Sun Solaris 10 (solo per piattaforma Intel)

### *SO Windows:*

*- 32 bit:*

Windows 98
Windows Millennium Edition
Windows NT4 (SP6a)
Windows 2000 Professional (SP4 anche con Update Rollup 1)
Windows 2000 Server (SP4 anche con Update Rollup 1)
Windows XP Professional (anche con SP1 e superiori)
Windows XP Home (anche con SP1 e superiori)
Windows Server 2003 (anche con SP1 e superiori)
Windows Vista (anche con SP1 e superiori)

Windows Server 2008 (anche con SP1 e superiori)
Windows 7
Windows 8

*- 64 bit:*

Windows Server 2003 (anche con SP1 e superiori)
Windows Vista (anche con SP1 e superiori)
Windows Server 2008 (anche con SP1 e superiori)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

### *SelfPROtect, SplDer Gate, Controllo Ufficio, FireWall*

*- 32 bit:*

Windows 2000 Professional (SP4 anche con Update Rollup 1)
Windows 2000 Server (SP4 anche con Update Rollup 1)
Windows XP Professional (anche con SP1 e superiori)
Windows XP Home (anche con SP1 e superiori)
Windows Server 2003 (anche con SP1 e superiori)
Windows Vista (anche con SP1 e superiori)
Windows Server 2008 (anche con SP1 e superiori)
Windows 7
Windows 8

*- 64 bit:*

Windows Server 2003 (anche con SP1 e superiori)
Windows Vista (anche con SP1 e superiori)
Windows Server 2008 (anche con SP1 e superiori)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

### *SO Windows Mobile*

Windows Mobile 2003
Windows Mobile 2003 Second Edition
Windows Mobile 5.0
Windows Mobile 6.0
Windows Mobile 6.1
Windows Mobile 6.5

### *SO Novell NetWare*

Novell NetWare 4.11 SP9
Novell NetWare 4.2
Novell NetWare 5.1
Novell NetWare 6.0
Novell NetWare 6.5

### *Mac OS X*

Mac OS 10.4 (Tiger)
Mac OS 10.4 Server (Tiger Server)
Mac OS 10.5 (Leopard)
Mac OS 10.5 Server (Leopard Server)
Mac OS 10.6 (Snow Leopard)
Mac OS 10.6 Server (Snow Leopard Server)
Mac OS 10.7 (Lion)

### *Android*

Android 1.6
Android 2.0
Android 2.1
Android 2.2

Android 2.3
Android 3.0
Android 3.1
Android 3.2
Android 4.0.

# Allegato B. Configurazioni, necessarie per utilizzo di DBMS. Configurazioni driver DBMS



La struttura del database di **Enterprise Server** si può ottenere sulla base di script sql `init.sql`, locato nella sottocartella `etc` della cartella di installazione di **Enterprise Server**.

Come il database di **Enterprise Server** può essere utilizzato:

- DMBS incorporato (IntDB);
- DBMS esterno.

## *DBMS incorporato*

Durante la configurazione di richiamo del DBMS incorporato per conservare e elaborare i dati si utilizzano i parametri, riportati nella tabella B-1.

**Tabella B-1. DBMS incorporato (IntDB)**

| Nome | Valore predefinito | Descrizione |
|---|---|---|
| `DBFILE` | `dbinternal.dbs` | Percorso al file di database |
| `CACHESIZE` | `2000` | Dimensione del cash di database in pagine |
| `SYNCHRONOUS` | `FULL` | Modalità scrittura sincrona di modifiche nel database sul disco:<br>• `FULL` — scrittura sul disco completamente sincrona,<br>• `NORMAL` — scrittura sincrona dei dati critici,<br>• `OFF` — scrittura asincrona |

## *DMBS esterno*

Come il database esterno di **Enterprise Server** può essere utilizzato:

- DBMS Oracle. La descrizione della configurazione è riportata in Allegato B2. Configurazione driver database per Oracle.
- DBMS Microsoft SQL Server Compact Edition (SQL CE). La descrizione della configurazione è riportata in Allegato B3. Configurazione driver database per SQL CE.
- DBMS PostgreSQL. La descrizione delle configurazioni, necessarie per DBMS PostgreSQL è riportata in Allegato B4. Utilizzo di DBMS PostgreSQL.
- Microsoft SQL Server/Microsoft SQL Server Express. Per accedere ai dati del DBMS, si può utilizzare il driver ODBC (configurazione parametri driver ODBC per il SO Windows è riportata in Allegato B1. Configurazione di driver ODBC).



Se si utilizza Microsoft SQL Server 2005, si richiede il driver ODBC, fornito con questo DBMS.

Si supporta utilizzo di Microsoft SQL Server 2005 (SP4) e superiori.

Si consiglia fortemente di installare ultimi aggiornamenti del server del database utilizzato.

Il database Microsoft SQL Server Express non è consigliabile se viene messa in funzione una rete antivirus con un numero grande di workstation (da 100 postazioni e più).

## *Caratteristici comparative*



Utilizzo del database interno è ammissibile alla connessione al **Server** di meno di 200-300 workstation. Se lo permette la configurazione hardware del computer, su cui è installato **Enterprise Server**, e il carico di altri processi, eseguiti su questo computer, si possono connettere fino a 1000 workstation.

Nel caso contrario si deve utilizzare il database esterno.

Se si utilizza il database esterno e al **Server** si connettono più di 10000 workstation si consiglia di eseguire i seguenti requisiti minimi:

- processore con frequenza 3 GHz,
- memoria operativa - da 4 GB per **Enterprise Server,** da 8 GB – per il server di database,
- SO della famiglia UNIX.

Se si sceglie tra database incorporato e database esterno si devono considerare alcuni parametri, caratteristici di ogni DBMS:

- Nelle grandi reti antivirus (più di 200-300 workstation) si consiglia di utilizzare un database esterno, più resistente ai malfunzionamenti di database incorporati.
- Se si utilizza il database incorporato non si richiede l'installazione dei componenti di fornitori terzi. Si consiglia durante utilizzo tipico.
- Il database incorporato non richiede conoscenze di amministrazione del DBMS ed è una buona scelta per la rete antivirus di dimensioni piccole e medie.

- Si può utilizzare il database esterno nel caso di lavoro autonomo con il database, che richiede un diritto accesso al database. In questo caso si possono utilizzare API standard per accedere ai database, come: OLE DB, ADO.NET o ODBC. Comunque si deve prendere in considerazione che al momento non esiste un driver ODBC per il DBMS Microsoft SQL CE. Ma il supporto di tecnologie ADO.NET, nonché della lingua LINQ, semplifica significativamente operazione nelle applicazioni di questo DBMS e permette di utilizzare tutte le possibilità di piattaforma .NET Framework, compreso il sistema di creazione dei report CrystalReports.

# Allegato B1. Configurazione driver ODBC

Durante il richiamo di DBMS esterno per conservare e elaborare i dati si utilizzano i parametri, riportati nella tabella B-2.

**Tabella B-2. ODBC (solo nella versione per Windows)**

| Nome | Valore predefinito | Descrizione |
|---|---|---|
| DSN | drwcs | Nome set dei dati |
| USER | drwcs | Nome utente |
| PASS | drwcs | Password |
| TRANSACTION | DEFAULT | v. sotto |

Valori disponibili del parametro TRANSACTION:

- SERIALIZABLE
- READ_UNCOMMITTED
- READ_COMMITTED
- REPEATABLE_READ
- DEFAULT

Valore predefinito DEFAULT significa "utilizzare impostazioni di default di server SQL". Per maggiori informazioni su livelli di isolamento di transazioni vedere la documentazioni del DBMS corrispondente.



Per escludere problemi con codifica, si devono disattivare i seguenti parametri di ODBC driver:

- **Utilizzare configurazioni nazionali** - potrebbe causare errori durante la formattazione dei parametri numerici.
- **Eseguire conversione dei dati di caratteri** - potrebbe causare la visualizzazione non corretta dei caratteri nel **Centro gestione** per i parametri, che provengono dal database. Imposta la dipendenza di visualizzazione dei caratteri dal parametro di lingua per i programmi, che non utilizzano Unicode.

Il database stesso si crea preliminariamente sul server SQL con i parametri, descritti sotto. **Si devono inoltre configurare i parametri del driver ODBC per il computer**, su cui è installato **Enterprise Server**. ***Per farlo:***

1. Nel **Pannello di controllo** del SO Windows scegliere la voce **Amministrazione**, nella finestra aperta fare il doppio click su icona **Fonti di dati (ODBC)**. Si apre la finestra **Amministrazione di fonti di dati ODBC**. Passare alla scheda **DSN di sistema**.
2. Premere sul tasto **Aggiungere**. Si apre la finestra di scelta del driver.
3. Scegliere nella lista la voce, corrispondente al driver ODBC per questo database, e premere sul tasto **Finito**. Si apre prima delle finestre di configurazione di accesso al server dei database.



Durante l'utilizzo del DBMS esterno si deve installare l'ultima versione del driver ODBC, fornita insieme a questo DBMS. Utilizzo del driver ODBC, fornito insieme al SO Windows, non è consigliato. Le esclusioni sono i database, forniti da Microsoft senza il driver ODBC.

4. Indicare i parametri di accesso a fonte di dati, corrispondenti con impostati nelle configurazioni di **Enterprise Server.** Se il server del database non si trova sullo stesso computer che **Enterprise Server**, indicare nel campo di input il **Server** e il suo indirizzo e nome. Premere sul tasto **Avanti**. Si apre la

finestra successiva di configurazione.

5. Inserire le configurazioni necessarie di accesso al database in questa finestra. Premere sul tasto **Configurazione di client**. Si apre la finestra di scelta e di configurazione del protocollo di rete.
6. Scegliere libreria per protocollo **TCP/IP** o **Named pipes** (consigliato). Se il server di database funziona non sul computer locale, impostare al posto del punto nei campi di input **Pseudonimo per server** e **Nome computer** il suo nome e indirizzo. Premere sul tasto **OK**. La finestra si chiude. Si torna nella finestra di configurazione del driver. Premere sul tasto **Avanti**. Si apre la finestra successiva di configurazione.
7. Assicurarsi che è scelta l'opzione **Solo alla disattivazione** e sono impostati i seguenti flag: **identificatori tra le virgolette nel formato ANSI**, **valori null**, **template e avvisi nel formato ANSI**. Premere sul tasto **Avanti**. Si apre l'ultima finestra di configurazione di accesso.



Se durante la configurazione del driver ODBC c'è possibilità di modificare la lingua dei messaggi di sistema del server SQL, si deve impostare l'inglese.

8. Al completamento della configurazione premere sul tasto **Finito**. Si apre la finestra con il riassunto dei parametri impostati.
9. Per controllare la correttezza delle configurazioni premere sul tasto **Controllare fonte dati**. Dopo l'avviso di controllo completato con successo premere sul tasto **OK**.

# Allegato B2. Configurazione driver database per Oracle

## *Descrizione generale*

Oracle Database (o Oracle DBMS) — è un DBMS relazionale ad oggetti. Oracle può essere utilizzata come database esterno per **Dr.Web ESS**.



**Enterprise Server** può utilizzare DBMS Oracle come database esterno su tutte le piattaforme, oltre FreeBSD (v. Installazione e versioni supportate).

***Per utilizzare DBMS Oracle è necessario:***

1. Installare una copia del database Oracle con configurazioni di codifica `AL32UTF8`. Si può inoltre utilizzare una copia esistente del database con codifica indicata.
2. Configurare driver del database per utilizzare database interno corrispondente. Si può farlo nel file di configurazione o con il **Centro gestione**: menu **Configurazione Dr.Web Enterprise Server**, scheda **Base di dati**.



Se si programma di utilizzare come database esterno Oracle, durante l'installazione (aggiornamento) del **Server**, nelle configurazioni di installazione scegliere la voce Installazione **personalizzata** e nella finestra successiva annullare installazione di client incorporato per DBMS Oracle (nella sezione **Supporto Database - driver database Oracle**).

Altrimenti l'operazione con il database Oracle via ODBC non sarà possibile per il conflitto di librerie.

## *Installazione e versioni supportate*

Per poter utilizzare database Oracle come database esterno si deve installare una copia del database Oracle e configurare su essa la codifica `AL32UTF8` (`CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16`). Si può farlo in seguenti modi:

1. Con installazione del database Oracle (utilizzare modalità avanzata di installazione e di configurazione del database).
2. Con il comando SQL `CREATE DATABASE`.

Le informazioni più dettagliate su creazione e configurazione del database sono riportate nella documentazione di Oracle database.



Se si utilizza codifica, diversa da quella indicata, i caratteri nazionali saranno visualizzati scorrettamente.

Il client per accedere al database (Oracle Instant Client) fa parte del kit di installazione di **Dr.Web ESS**.

Le piattaforme, supportate da DBMS Oracle, sono riportate sul sito del produttore http://www.oracle.com/technology/software/tech/oci/instantclient/index.html.

**Dr.Web ESS** supporta le seguenti versioni del DBMS: Oracle9i Database Release 2: 9.2.0.1 - 9.2.0.8 e superiori.

## *Parametri*

Durante la configurazione del richiamo del DBMS Oracle si utilizzano i parametri, descritti nella tabella B-3.

**Tabella B-3. Parametri del DBMS Oracle**

| Parametro | Descrizione |
|---|---|
| `drworacle` | Nome driver |
| `User` | Nome utente del database (obbligatorio) |
| `Password` | Password utente (obbligatorio) |
| `ConnectionString` | Riga di connessione al database (obbligatorio) |

***Il formato di riga di connessione al DBMS è il seguente:***

*//<host>:<porta>/<nome servizio>*

dove:

- *<host>* - indirizzo IP o nome del server Oracle;
- *<porta>* - porta, che "ascolta" server;
- *<nome servizio>* - nome del database, a cui si deve connettersi.

**Per esempio:**
`//myserver111:1521/bjava21`

dove:

- `myserver111` - nome del server Oracle.
- `1521` - porta, che "ascolta" Server.
- `bjava21` - nome del database, a cui si deve connettersi.

## *Esempio di file di configurazione drwcsd.conf*

Per usare il DBMS Oracle, è necessario modificare la definizione e le impostazioni del driver del database in uno dei seguenti modi:

- nel **Centro gestione**: la voce **Amministrazione** del menu principale → la voce **Configurazione Dr.Web Enterprise Server** del menu di gestione → la scheda **Base di dati** → selezionare dalla lista a cascata **Base di dati** il tipo **Oracle**, impostare i parametri secondo il formato riportato sopra.
- nel file di configurazione di **Server**. Un frammento del file di configurazione con i parametri corrispondenti è riportato di seguito:

```
...
;Database definition. Mandatory.
;Only one definition is allowed.
database


;DB driver (DLL or shared object name)
drworacle  ; Oracle DB, unix & windows


;load library from this path; empty - use default
from ""
```

```
using "User=DRWCS Password=root
ConnectionString=//192.168.0.1:1521/ORADB"
```

# Allegato B3. Configurazione database driver per SQL CE



Si consiglia di utilizzare il database incorporato invece del database MS SQL CE, se non è necessaria operazione indipendente con il database via ADO.NET. Il database è caratterizzato da elevata stabilità e produttività rispetto a MS SQL CE.

## *Descrizione generale*

Microsoft SQL Server Compact Edition (SQL CE) — è un database relazionale della società Microsoft. Rappresenta un database incorporato per le applicazioni desktop e utenze mobili. SQL CE può essere utilizzata come database esterno per **Dr.Web ESS.**

### *Per utilizzare SQL Server CE è necessario:*

1. Installare il server SQL CE.
2. Configurare il driver del database su utilizzo del database esterno corrispondente. Si può farlo nel file di configurazione o con il **Centro gestione**: menu **Configurazione Dr.Web Enterprise Server**, scheda **Base di dati**.

## *Installazione e piattaforme supportate*



DBMS SQL CE supporta sistemi operativi Windows 2000 e superiori (nelle versioni per x32 e x64).

**Dr.Web Enterprise Security Suite** supporta SQL CE delle versioni 3.5 SP1/SP2 per piattaforme x64 e x86. La compatabilità con le versioni successive del database SQL CE non è garantita.

Per poter utilizzare il database SQL Server Compact Edition si deve scaricare il set di installazione dal sito del produttore http://www.microsoft.com/sqlserver/2005/en/us/compact-downloads.aspx e installare il server della versione corrispondente (v. anche Requisiti di sistema per la versione 3.5.).



Non si consiglia di installare più di una versione di SQL Server Compact per eventuali problemi di compatibilità.

I database, creati nelle varie versioni di SQL Server Compact possono essere non compatibili, siccome la versione 3.1, a differenza della versione 3.5, non supporta codifica. Quindi, se è necessario cambiare la versione, il trasloco del database deve essere eseguito solo con i comandi di **Dr.Web Enterprise Security Suite** `exportdb` o `importdb`.

Il client per accedere al database fa parte del kit di installazione di **Dr.Web ESS**.

## *Parametri*

Durante la configurazione del richiamo del DBMS SQL CE si utilizzano i parametri, descritti nella tabella B-4.

**Tabella B-4. Parametri DBMS SQL CE**

| Parametro | Descrizione |
|---|---|
| `drwsqlce` | Nome driver. |
| `DBFILE` | Nome database (predefinito `mssqlce.sdf`). |
| `PASSWORD` | Password, utilizzato per codificare database. |

Il parametro PASSWORD è una chiave di codifica e non c'entra con il sistema password/utente.

Di default la password è vuoto (il database non viene codificato).

## *Esempio di file di configurazione drwcsd.conf*

Con utilizzo di SQL CE si devono modificare definizione e configurazioni del database nel file di configurazione di **Enterprise Server**. Un frammento di file di configurazione con i parametri corrispondenti è riportato di seguito:

```
...
;Database definition. Mandatory.
;Only one definition is allowed.
database


;DB driver (DLL or shared object name)
drwsqlce  ; sql server compact, windows only


;load library from this path; empty - use default
from ""
;parameters describing database connection
;defaults (DBFILE: varroot/mssqlce.sdf)
;using "DBFILE=mssqlce.sdf PASSWORD=drwcs"
using "DBFILE=mssqlce.sdf PASSWORD=drwcs"
```

# Allegato B4. Utilizzo di DBMS PostgreSQL

## *Descrizione generale*

PostgreSQL è un DBMS relazionale ad oggetti. È un'alternativa libera a DBMS commerciali (come Oracle Database, Microsoft SQL Server ecc). Nelle grandi reti antivirus il DBMS PostgreSQL può essere utilizzato come il database esterno per **Dr.Web ESS**.

Per questo è necessario:

1. Installare il server PostgreSQL.
2. Configurare il driver ODBC.
3. Configurare **Enterprise Server** a utilizzare il database esterno corrispondente. Si può farlo nel file di configurazione o con il **Centro gestione**: menu **Configurazione Dr.Web Enterprise Server**, scheda **Base di dati**.

## *Installazione e versioni supportate*

Scaricare ultima versione del prodotto gratuito PostgreSQL (server PostgreSQL e driver ODBC corrispondente) o almeno non utilizzare versione inferiore a 8.2.



DBMS PostgreSQL esiste in realizzazioni per seguenti piattaforme: Linux, Solaris/OpenSolaris, Win32, MacOS X, FreeBSD.

Per le informazioni utili su installazione e utilizzo di PostgreSQL con **Enterprise Server** v. qui.

Questo articolo descrive in dettagli la creazione del database esterno PostgreSQL e installazione di **Dr.Web Enterprise Security Suite** con utilizzo di database creato in precedenza. Se c'è **Dr.Web Enterprise Security Suite** installato, creazione del database PostgreSQL viene eseguito nello stesso modo, e il passaggio al

database esterno è descritto in dettagli in Cambio tipo DBMS Dr.Web Enterprise Suite.



Versione ANSI del driver ODBC può essere utilizzata solamente partendo dalla versione PostgreSQL 8.2.4. Driver ODBC per Unicode funziona normalmente in tutte le versioni.

### *Installazione su sistemi a 64 bit*

Il driver psqlODBC per i SO a 64 bit non è ufficialmente fornito da sviluppatore. Comunque, secondo il sito ufficiale del DBMS PostgreSQL, si possono installare i pacchetti di installazione prerilasciati che si possono scaricare, per esempio, ai seguenti link:

- http://www.enterprisedb.com/products/pgdownload.do#windows
- http://code.google.com/p/visionmap/wiki/psqlODBC
- http://www.geocities.jp/inocchichichi/psqlodbc/index.html



Dopo installazione di driver ODBC su SO a 64 bit, per poter accedere ai driver, utilizzare il pannello di controllo amministrativo, locato qui: `C:\WINDOWS\SYSWOW64\odbcad32.exe`.

## *Parametri*

Durante la configurazione del richiamo del database PostgreSQL si utilizzano i parametri, descritti nella tabella B-5.

**Tabella B-5. PostgreSQL (solo nella versione per il SO UNIX)**

| Nome | Valore predefinito | Descrizione |
|---|---|---|
| `host` | *<socket UNIX locale>* | Host del server PostgreSQL |

| Nome | Valore predefinito | Descrizione |
|---|---|---|
| `port` | | Porta del server PostgreSQL o estensione di nome di file di socket |
| `dbname` | `drwcs` | Nome database |
| `user` | `drwcs` | Nome utente |
| `password` | `drwcs` | Password |
| `options` | | Opzioni debugging/tracing per inviare al server |
| `tty` | | File o `tty` per output durante debugging |
| `requiressl` | | 1 per richiesta di stabilimento di connessione SSL o 0 per assenza di richiesta |

Le informazioni tecniche si possono inoltre ottenere all'indirizzo http://www.postgresql.org/docs/manuals/.

## *Interazione di Dr.Web Enterprise Server con database PosrtgreSQL via UDS*

Durante installazione di **Enterprise Server** e del database PostgreSQL su una workstation è disponibile la configurazione di interazione di essi via UDS (socket di dominio di UNIX).

***Per configurare operazione via UDS è necessario:***

1. Nel file di configurazione del database PostgreSQL `postgresql.conf` prescrivere la seguente directory per UDS:

   ```
   unix_socket_directory = '/var/run/postgresql'
   ```

2. Riavviare PostgreSQL.

# Allegato C. Descrizione parametri sistema di avvisi

Durante la configurazione del sistema di avvisi degli eventi, legati all'operazione dei componenti della rete antivirus, per i vari tipi di driver del plugin di avvisi vengono utilizzati i parametri, descritti di seguito.

**Tabella C-1. Avvisi per posta elettronica (driver drwemail)**

| Parametro | Valore predefinito | Descrizione |
|---|---|---|
| HOST | 127.0.0.1 | Host del server SMTP |
| PORT | 25 | Porta del server SMTP |
| PASS | | Password SMTP |
| USER | | SMTP utente |
| DEBUG | NO | Modalità di debugging |
| FROM | drwcsd@localhost | Indirizzo mittente |
| TO | root@localhost | Indirizzo destinatario |

**Tabllea C-2. Avviso con utilizzo di Windows Messenger (driver drwwnetm), solo nella versione per i SO Windows**

| Parametro | Valore predefinito | Descrizione |
|---|---|---|
| TO | Admin | Nome di rete del computer |



Sistema di avvisi per la rete Windows è operativo solamente nei SO Windows con il supporto del servizio Windows Messenger (Net Send).

Il SO Windows Vista e superiori non supportano il servizio Windows Messenger.

# Allegato D. Parametri modelli sistema di avvisi

Testi di messaggi (per posta elettronica o via **Windows Messenger**) si generano dal componente del **Server**, chiamato il processore di modelli, sulla base del file di modelli.



Sistema di avvisi per la rete Windows è operativo solamente nei SO Windows con il supporto del servizio Windows Messenger (Net Send).

Il SO Windows Vista e superiori non supportano il servizio Windows Messenger.

File di modello contiene testo e variabili nelle parentesi graffe. Durante la modifica dei file di modelli si possono utilizzare le variabili, riportate sotto.



Il processore di modelli non utilizza le sostituzioni recursive.

***I variabili si scrivono in uno dei seguenti modi:***

- {<*VAR*>} – sostituire direttamente il valore della variabile <*VAR*>.
- {<*VAR*>:<*N*>} – primi <*N*> caratteri di variabile <*VAR*>.
- {<*VAR*>:<*first*>:<*N*>} – <*N*> caratteri di variabile <*VAR*>, che seguono dopo i <*first*> primi (partendo dal <*first*>+1-o carattere), se il resto è di meno - si aggiungono degli spazi a destra.
- {<*VAR*>:<*first*>:-<*N*>} – <*N*> caratteri di variabile <*VAR*>, che seguono dopo i <*first*> primi (partendo dal <*first*>+1-o carattere), se il resto è di meno - si aggiungono degli spazi a sinistra.

- {*<VAR>*/*<original1>*/*<replace1>*[/*<original2>*/*<replace2>*]} – sostituzione di caratteri indicati di variabile *<VAR>* con i valori indicati: caratteri *<original1>* si sostituiscono con i caratteri *<replace1>*, se ci sono caratteri *<original2>* si sostituiscono con i caratteri *<replace2>* ecc.

  Non ce ne sono limitazioni della quantità di paia di sostituzione.

**Tabella D-1. Modo registrazione variabili**

| Variabile | Valore | Espressione | Risultato |
|---|---|---|---|
| SYS.TIME | 10:35:17:456 | {SYS.TIME:5} | 10:35 |
| SYS.TIME | 10:35:17:456 | {SYS.TIME:3:5} | 35:17 |
| SYS.TIME | 10:35:17:456 | {SYS.TIME:3:-12} | °°°35:17:456 |
| SYS.TIME | 10:35:17:456 | {SYS.TIME:3:12} | 35:17:456°°° |
| SYS.TIME | 10:35:17:456 | {SYS.TIME/10/99/35/77} | 99:77:17:456 |

**Segni convenzionali**

° - carattere di spazio.

## *Variabili di sistemi:*

- `SYS.TIME` — ora del sistema attuale,
- `SYS.DATE` — data del sistema attuale,
- `SYS.DATETIME` — data e ora del sistema attuali,
- `SYS.VERSION` — versione del **Server**,
- `SYS.BUILD` — data del build del **Server**,
- `SYS.PLATFORM` — piattaforma del **Server**,
- `SYS.PLATFORM.SHORT` — variante breve di `SYS.PLATFORM`,
- `SYS.OS` — nome del sistema operativo del computer con il **Server** installato,
- `SYS.BRANCH` — versione di **Agent** e di **Server**,

- `SYS.SERVER` — nome del prodotto (**Dr.Web Enterprise Server**).

Variabili di ambiente hanno gli stessi nomi delle varibili definite in ambiente, con il prefisso `ENV` aggiunto. (prefisso finisce con il punto).

### *Variabili generali dei messaggi, Agent:*

- `GEN.LoginTime` — tempo di connessione di workstation,
- `GEN.StationAddress` — indirizzo di workstation,
- `GEN.StationID` — UUID di workstation,
- `GEN.StationName` — nome di workstation.

### *Variabili generali dei messaggi, sottosistema di aggiornamento del Server:*

- `GEN.CurrentRevision` — identificatore attuale della versione,
- `GEN.NextRevision` — identificatore della versione aggiornata,
- `GEN.Folder` — cartella del location del prodotto,
- `GEN.Product` — descrizione del prodotto.

### *Variabili dei messaggi, per messaggi (per Agent):*

**`Administrator_Authorization_Failed`:**

- `MSG.Login` — nome di utenza,
- `MSG.Address` — indirizzo di rete del **Centro gestione**;

**`Approved_Newbie`:**

- `MSG.AdminName` — nome dell'amministratore,
- `MSG.AdminAddress` — indirizzo del **Centro gestione**;

**`AutoApproved_Newbie`**: variabili sono assenti;

**Awaiting_Approval**: variabili sono assenti;

**Cannot_Add_Station:**

- MSG.ID — UUID di workstation;

**Connection_Terminated_Abnormally:**

- MSG.Reason — ragione della terminazione;

**Infection:**

- MSG.Component — nome del componente,
- MSG.RunBy — utente, da cui nome è avviato il componente,
- MSG.ServerTime — tempo di ricezione dell'evento, GMT,
- MSG.ObjectName — nome dell'oggetto infetto,
- MSG.ObjectOwner — proprietario dell'oggetto infetto,
- MSG.InfectionType — tipo di infezione,
- MSG.Virus — nome del virus,
- MSG.Action — azione, applicata al rilevamento;

**Installation_Bad:**

- MSG.Error — messaggio di errore;

**Installation_OK:** variabili sono assenti;

**License_Limit** — viene inviato, quando il numero di workstation registrate avvicina alla limitazione di licenza, cioè: non è utilizzato meno del 5% del limite di licenza o meno di due workstation:

- MSG.Used — numero di workstation nel database,
- MSG.Licensed — consentito da licenza;

**Low_Var_Free_Space:**

- MSG.Path — percorso alla cartella con il basso volume di memoria,
- MSG.FreeSpace — spazio libero in byte,
- MSG.FreeInodes — numero di descrittori di file inodes liberi (valido solo per alcuni sistemi della famiglia UNIX),
- MSG.RequiredSpace — volume della memoria libera,

necessario per l'operazione,

- `MSG.RequiredInodes` — numero di inodes liberi, necessario per l'operazione (valido solo per alcuni sistemi della famiglia UNIX);

**`Near_Max_Stations`** (viene avviato durante ogni avvio del **Server** nel caso, se **Server** è avviato con la chiave di licenza che prevede il numero di licenze per le workstation inferiore al numero di workstation connesse al **Server**):

- `MSG.Used` — numero workstation in database,
- `MSG.Licensed` — consentito da licenza,
- `MSG.Percent` — percentuale delle licenze disponibili;

**`Newbie_Not_Allowed`**: variabili sono assenti;

**`Not_Seen_For_A_Long_Time`:**

- `MSG.StationName` — nome di workstation,
- `MSG.StationID` — UUID di workstation,
- `MSG.DaysAgo` — numero di giorni dal momento di ultima connessione al **Server**,
- `MSG.LastSeenFrom` — indirizzo, da cui la workstation è connessa al **Server** l'ultima volta;

**`Processing_Error`:**

- `MSG.Component` — nome del componente,
- `MSG.RunBy` — utente, da cui nome è avviato il componente,
- `MSG.ServerTime` — tempo di ricezione dell'evento, GMT,
- `MSG.ObjectName` — nome di oggetto,
- `MSG.ObjectOwner` — proprietario di oggetto,
- `MSG.Error` — messaggio di errore;

**`Rejected_Newbie`:**

- `MSG.AdminName` — nome dell'amministratore,
- `MSG.AdminAddress` — indirizzo del **Centro gestione**;

**`Station_Already_Logged_In`** – viene inviato, se la

workstation è già attualmente registrata su questo o su altro **Server**:

- `MSG.ID` — UUID di workstation,
- `MSG.StationName` — nome di workstation,
- `MSG.Server` — ID del **Server**, su cui workstation è registrata,

**`Station_Authorization_Failed`**:

- `MSG.ID` — UUID di workstation,
- `MSG.Rejected` — valore `rejected` — a workstation è stato negato accesso, `newbie` — è stato fatto il tentativo di passare la workstation allo stato "nuova";

**`Statistics`**:

- `MSG.Component` — nome del componente,
- `MSG.ServerTime` — tempo di ricezione dell'evento, GMT,
- `MSG.Scanned` — numero di oggetti scansionati,
- `MSG.Infected` — numero di oggetti infetti,
- `MSG.Modifications` — numero di oggetti, infetti dai virus modificati,
- `MSG.Suspicious` — numero di oggetti sospetti,
- `MSG.Cured` — numero di oggetti curati,
- `MSG.Deleted` — numero di oggetti eliminati,
- `MSG.Renamed` — numero di oggetti rinominati,
- `MSG.Moved` — numero di oggetti spostati,
- `MSG.Speed` — velocità di elaborazione in kB/sec;

**`Too_Many_Stations`** — viene inviato, quando una nuova workstation non può registrarsi sul **Server** per le limitazioni di licenza:

- `MSG.ID` — UUID di workstation,

**`Unknown_Administrator`**:

- `MSG.Login` — nome di utenza,
- `MSG.Address` — indirizzo di rete del **Centro gestione**.

**`Unknown_Station`**:

- `MSG.ID` — UUID di workstation sconosciuta,
- `MSG.Rejected` — valore `rejected` — a workstation è stato negato accesso, `newbie` — è stato fatto il tentativo di passare la workstation allo stato "nuova";

**`Update_Failed`:**

- `MSG.Product` — prodotto aggiornato,
- `MSG.ServerTime` — ora (locale) di ricezione del messaggio dal **Server**;

**`Update_Wants_Reboot`:**

- `MSG.Product` — prodotto aggiornato,
- `MSG.ServerTime` — ora (locale) di ricezione del messaggio dal **Server**.

### *Variabili di avvisi, per avvisi (per sottosistema di aggiornamento del Server):*

**`Srv_Repository_Cannot_flush`**: variabili sono assenti;

**`Srv_Repository_UpToDate`**: variabili sono assenti;

**`Srv_Repository_Frozen`**: variabili sono assenti;

**`Srv_Repository_Load_failure`**:

- `MSG.Reason` — avviso di ragione di errore;

**`Srv_Repository_Update`:**

- `MSG.AdddedCount` — numero di file aggiunti,
- `MSG.ReplacedCount` — numero di file sostituiti,
- `MSG.DeletedCount` — numero di file eliminati,
- `MSG.Added` — lista di file aggiunti (ogni nome in una riga separata),
- `MSG.Replaced` — lista di file sostituiti (ogni nome in una riga separata),

- `MSG.Deleted` — lista di file eliminati (ogni nome in una riga separata).

**`Srv_Repository_UpdateFailed`:**

- `MSG.Error` — avviso di errore,
- `MSG.ExtendedError` — descrizione dettagliata di errore.



Variabili dell'ultimo modello non comprendono i file, marcati come "**ignorati in avvisi**" nel file di configurazione del prodotto, v. F1. Sintassi file di configurazione .config.

## *Variabili di avviso del Server della scadenza vicina del periodo di validità di licenza:*

**`Key_Expiration`:**

- `MSG.Expiration` — data di scadenza di licenza,
- `MSG.Expired` — 1, se il periodo di validità è già scaduto, altrimenti - 0,
- `MSG.ObjId` — GUID di oggetto,
- `MSG.ObjName` — nome di oggetto,
- `MSG.ObjType` — oggetto, che utilizza la chiave scadente (`server/station/group`).

# Allegato E. Specifica di indirizzo di rete

In questa specifica si utilizzano le seguenti designazioni:

- variabili (campi da sostituire con i valori concreti) si racchiudono fra parentesi angolate e si scrivono in corsivo,
- testo costante (che rimane dopo le sostituzioni) viene scritto con font monospaziato,
- elementi non obbligatori si racchiudono fra parentesi quadre,
- a sinistra di stringa dei caratteri `::=` si trova il termine definito, a destra — definizione (come nel Backus Naur Form).

## E1. Formato generale di indirizzo

Indirizzo di rete ha il seguente aspetto:
`[`*<protocollo>*`/][`*<parte-specifica-protocollo>*`]`

Di default *<protocollo>* ha il valore `TCP`. Sono possibile anche `IPX` e `NetBIOS`. I valori predefiniti *<parte-specifica-protocollo>* sono definiti dall'applicazione.

### Indirizzi della famiglia IP

- *<interfaccia>*`::=`*<indirizzo-ip>*

  *<indirizzo-ip>* può essere nome DNS o indirizzo IP, separato da punti (per esempio, `127.0.0.1`).

- *<indirizzo-socket>*`::=`*<interfaccia>*`:`*<numero-porta>*

  *<numero-porta>* deve essere impostato dal numero decimale.

### Indirizzi della famiglia IPX

- *<interfaccia>*`::=`*<rete-ipx>*`.`*<indirizzo-mac>*

  *<rete-ipx>* deve contenere 8 cifre esadecimali, *<indirizzo-mac>*

deve contenere 12 cifre esadecimali.

- *<indirizzo-socket>*`::=`*<interfaccia>*`:`*<numero-socket>*

  *<numero-socket>* deve contenere 4 cifre esadecimali.

## Indirizzi della famiglia NetBIOS

- Protocollo orientato al datagramma:

  `nbd/<NOME>[:<PORTA>[:<LANA>]]`

- Protocollo orientato alla connessione:

  `nbs/<NOME>[:<PORTA>[:<LANA>]]`

  dove *<NOME>* — nome NetBIOS del computer, *<PORTA>* — porta (predefinita `23`), *<LANA>* — numero adattatore di rete (rilevante per NetBEUI).

**Esempi:**

`1.tcp/127.0.0.1:2193`

significa protocollo `TCP`, porta `2193` su interfaccia `127.0.0.1`.

`2.tcp/[::]:2193`

significa protocollo `TCP`, porta `2193` su interfaccia IPv6 `0:0:0:0:0:0:0:0`

`3.localhost:2193`

uguale.

`4.tcp/:9999`

valore per server: interfaccia predefinita, che dipende da applicazione (di solito tutte le interfacce disponibili), porta `9999`; valore per client: connessione a host predefinito, che dipende da applicazione (di solito localhost), porta `9999`.

`5.tcp/`

protocollo `TCP`, porta predefinita.

`6.spx/00000000.000000000001:2193`

significa socket `SPX loopback 0x2193`.

## Indirizzi della famiglia UDS

- Protocollo orientato alla connessione:
  `unx/`*<nome_file>*
- Protocollo orientato al datagramma:
  `udx/`*<nome_file>*

**Esempi:**

1. `unx/tmp/drwcsd:stream`
2. `unx/tmp/drwcsd:datagram`

## Protocollo orientato alla connessione

*<protocollo>*`/`*<indirizzo-socket>*

dove *<indirizzo-socket>* imposta indirizzo locale di socket per server o server remoto per client.

## Protocollo orientato al datagramma

*<protocollo>*`/`*<indirizzo-socket-endpoint>*`[-`*<interfaccia>*`]`

**Esempi:**

1. `udp/231.0.0.1:2193`

   significa utilizzo del gruppo multicast `231.0.0.1:2193` su interfaccia che dipende da applicazione di default.
2. `udp/[ff18::231.0.0.1]:2193`

significa utilizzo del gruppo multicast `[ff18::231.0.0.1]` su interfaccia che dipende da applicazione di default.

3. `udp/`

   endpoint e interfaccia dipendente dall'applicazione

4. `udp/255.255.255.255:9999-`*<myhost1>*

   utilizzo di messaggi broadcast su porta `9999` in interfaccia *<myhost1>*.

# E2. Indirizzi di Dr.Web Enterprise Server

## Accettazione connessioni

*<protocollo-connessione>*`/[`*<indirizzo-socket>*`]`

Di default, a seconda di *<protocollo-connessione>*:

- `tcp/0.0.0.0:2193`

  che significa "tutte le interfacce (escluse quelle con indirizzi IPv6 assegnati), porta `2193`";

- `tcp/[::]:2193`

  che significa "tutte le interfacce IPv6, porta `2193`";

- `spx/00000000.000000000001:2193`

  che significa "tutte le interfacce, porta `0x2193`";

- `nbs/drwcs:23:0`

  che significa utilizzo del protocollo NetBIOS stream, porta `23`, computer `drwcs`.

## Servizio rilevamento di Dr.Web Enterprise Server

*<protocollo-datagramma>*/[*<indirizzo-socket-endpoint>*[-*<interfaccia>*]]

Di default, a seconda di *<protocollo-datagramma>*:

- udp/231.0.0.1:2193-0.0.0.0

  che significa utilizzo di gruppo multicast 231.0.0.1:2193 in tutte le interfacce;

- udp/[ff18::231.0.0.1]:2193-[::]:0

  che significa utilizzo del gruppo multicast [ff18::231.0.0.1:2193] in tutte le interfacce;

- ipx/00000000.FFFFFFFFFFFF:2193-00000000.000000000000

  che significa accettazione di messaggi broadcast su socket 0x2193 in tutte le interfacce;

- nbd/drwcs:23:0

  che significa utilizzo del protocollo datagramma NetBIOS, porta 23, computer drwcs.

# E3. Indirizzi di Dr.Web Enterprise Agent/ Installer

## Connessione diretta a Dr.Web Enterprise Server

[*<protocollo-connessione>*]/[*<indirizzo-socket-remoto>*]

Di default, a seconda di *<protocollo-connessione>*:

- tcp/127.0.0.1:2193

dove `127.0.0.1` - loopback, `2193` - porta;

- `tcp/[::1]:2193`

  dove `[::1]` - loopback (IPv6), `2193` - porta;

- `spx/00000000.000000000001:2193`

  dove `00000000.000000000001` - loopback, `2193` - porta.

## Ricerca del Server <drwcs-name>, che utilizza questa famiglia di protocolli ed endpoint

`[`*<nome-drwcs>*`]@`*<protocollo-datagrama>*`/[`*<indirizzo-socket-endpoint>*`[-`*<interfaccia>*`]]`

Di default, a seconda di *<protocollo-datagramma>*:

- `drwcs@udp/231.0.0.1:2193-0.0.0.0`

  ricerca del **Server** con il nome `drwcs` per connessione TCP, che utilizza il gruppo multicast `231.0.0.1:2193` in tutte le interfacce,

- `drwcs@ipx/00000000.FFFFFFFFFFFF:2193-00000000.000000000000`

  ricerca del **Server** con il nome `drwcs` per connessione SPX, utilizzando messaggi broadcast su socket `0x2193` in tutte le interfacce.

# Allegato F. Gestione repositorio

Gestione delle funzioni del repositorio dei prodotti si esegue con i seguenti file locati nella radice di cartella del prodotto:

- File di configurazione `.config`. Imposta contenuti dei file e parametri del server di aggiornamenti. File ha il formato del file di testo, la sua struttura si descrive sotto in Allegati F1. Sinstassi file di configurazione .config e F2. Significato istruzioni file .config.
- File di stato `.id`. Rispecchia lo stato generale del prodotto (numero di revisione e il passo di esecuzione di transazione). Il formato si descrive sotto in Allegato F3. File .id.



Durante la configurazione di connessioni intra-server (v. Particolarità rete con più Server) per fare lo specchio di prodotti si deve considerare che i file di configurazione non fanno parte del prodotto e non vengono elaborati dal sistema di creazione di specchi. Per evitare malfunzionamenti in operazione del sistema di aggiornamento:

- sui **Server** "alla pari" conservare la stessa configurazione,
- sui **Server** slave disattivare la sincronizzazione dei componenti via protocollo HTTP o conservare la stessa configurazione.



Dopo la modifica dei file di configurazione e file di stato si richiede il riavvio del **Server**.

# F1. Sintassi di file di configurazione .config

Durante la descrizione del formato di file di configurazione `.config` si utilizza grammatica formale, che si basa sulla notazione EBNF e comprende le seguenti simboli:

- `(...)` — gruppo dei simboli (frammento del file di configurazione),
- `"..."` — simbolo terminale;
- `<...>` — simbolo nonterminale;
- `|` – simbolo di scelta di uno di elementi proposti;
- `(...)?` – simbolo (o gruppo di simboli tra parentesi) a sinistra di operatore non è obbligatorio (può essere ripetuto 0 o 1 volta);
- `(...)*` – simbolo (o gruppo di simboli tra parentesi) a sinistra di operatore può essere ripetuto qualsiasi numero di volte (nonché può essere omesso);
- `(...)+` – simbolo (o gruppo di simboli tra parentesi) a sinistra di operatore può essere ripetuto 1 o più volte;
- `[...]` – qualsiasi simbolo, che rientra nel range indicato;
- punto alla fine — simbolo speciale, che indica che la regola è completata.

***Formato di file di configurazione del repositorio .config:***

```
<riga> := <istruzione>? (<separatore>+ <commento>?)*.

<istruzione> := <nome> "{"? <parametro>* "}"?.
<nome> := "description" | "sync-with" |
              "sync-delay" |  "sync-only" |
              "sync-ignore" | "state-only" |
              "state-ignore" | "notify-only" |
              "notify-ignore" | "notify-off".
<parametro> := <testo>.
<testo> := <parola> <separatore>*.
<parola> := (<simbolo> | <segno>)+.
<simbolo> := [a-zA-Z] | [0-9].
```

```
<segno> := "" | "/"| "\" | "*" | "^" | "." | "-"| "$".

<separatore> := \r | \t | \n | \s.

<commento> := ";"<testo> | "#"<M1><simbolo>+<M1> | "'"<M2><testo>+<M2>.
<M1> := <simbolo>+.
<M2> := <segno>+.
```

File di configurazione rappresenta una conseguenza di parole, separate uno dall'altro da separatori. Il *separatore* è una qualsiasi conseguenza dei seguenti simboli: spazio (`\s`), tabulazione (`\t`), ritorno del carrello (`\r`), nuova riga (`\n`).

Parola, che inizia con punto e virgola `(;)`, significa inizio commento, che dura fino alla fine di riga.

**Esempio:**

```
ghgh 123 ;questo è un commento
123;questo; non è; un commento - è necessario
      un separatore all'inizio.
```

Una parola, che inizia con il segno `(#)`, significa inizio del commento di flusso; il resto della parola imposta il marcatore di fine commento.

**Esempio:**

```
123 456 #COMM Da qui commentoCOMM già finito
```

Per includere in parola qualsiasi simbolo si utilizza il prefisso ' (apostrofo) — simbolo-separatore speciale per questa parola (cioè, proprio questo simbolo viene considerato separatore, che completa questa parola).

**Esempio:**

```
xy123 '*Ecco una parola*GiàUnAltra
```



Se parola inizia con uno dei simboli: apostrofo, punto e virgola, segno (', ;, #), - deve necessariamente essere limitata da simboli-separatori speciali, come indicato sopra.

`Il file .config` consiste di commenti e di istruzioni. L'ordine di conseguenza di istruzioni non è importante.



Il formato di istruzioni dei file di configurazione prevede distinzione tra caratteri minuscoli e maiuscoli.

Il repositorio distingue tra minuscoli e maiuscoli nonostante il file system e i SO, in cui opera il **Server**.

Significato di istruzioni è descritto in Allegato F2. Significato instruzioni del file .config.

# F2. Significato istruzioni del file .config

## *Istruzione description*

Istruzione `description` imposta il nome del prodotto, visualizzato nel **Centro gestione**. Se questa istruzione è assente, come nome di prodotto viene utilizzato il nome del catalogo corrispondente del prodotto.

**Esempio:**

```
description '"Dr.Web® Enterprise Agent"
```

## *Istruzione sync-with*

Istruzione `sync-with` imposta la lista dei server HTTP e server proxy HTTP per aggiornamento. Il parametro `name` imposta nome di dominio o indirizzzo IP. La costruzione `:port` può essere assente, in

tal caso di default il numero di porta è considerato `80` per server HTTP e `3128` per server proxy.

I server nella lista vengono richiesti di conseguenza, se l'aggiornamento completa con successso, la procedura di richiesta viene completata.



Nella versione corrente di **Dr.Web Enterprise Security Suite** è supportata solo l'autorizzazione HTTP di base, l'autorizzazione HTTP proxy e l'autorizzazione RADIUS.

Redirect HTTP costanti (sotto codice 301) si memorizzano nella cache di memoria fino al riavvio del server.

**Esempio:**

```
sync-with{
 http{ esuite.msk3.drweb.com /update }
 http{ esuite.msk4.drweb.com /update }
 http{ esuite.msk.drweb.com  /update }
 http{ esuite.us.drweb.com   /update }
 http{ esuite.jp.drweb.com   /update }
}
```

**Esempio con utilizzo di server proxy**

```
sync-with{
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.msk7.drweb.com /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.jp.drweb.com   /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.msk5.drweb.com /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.msk6.drweb.com /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.msk.drweb.com  /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
```

```
{ esuite.us1.drweb.com  /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.msk3.drweb.com /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.msk4.drweb.com /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.us.drweb.com   /update  } }
 http-proxy{   10.3.0.74   auth   user:pass   http
{ esuite.fr1.drweb.com  /update  } }
}
```

Dove:

- `10.3.0.74` - indirizzo IP del server proxy;
- `user` - nome utente del server proxy (può essere assente, se per proxy non è richiesta autenticazione);
- `pass` - password per accedere al server proxy (può essere assente, se proxy non richiede autenticazione).

## *Istruzione sync-only*

Istruzione `sync-only` imposta esplicitamente un insieme dei nomi di file (impostati sia con espressioni regolari in forma semplice, come visualizzato in questa sezione, sia in forma completa `qr{}`, come visualizzato in Avvio e arresto di scanner antivirus su workstation), che sono da sincronizzare. Se le istruzioni sono assenti, dei default da sincronizzare sono tutti i contenuti del catalogo (eslusi i file, i cui nomi iniziano con punto).

**Esempio:**

```
sync-only{^common/drw.*vdb$}
```

prescrive di aggiornare solamente i database dei virus.

## Istruzione sync-ignore

Istruzione `sync-ignore`, invece, esplicitamente imposta un insieme dei file, che non sono da sincronizzare.



Se nel prodotto sono stati aggiunti dei file localmente (che non sono presenti in originale) e instruzione sync-only non viene utilizzata, i file aggiunti devono essere elencati in `sync-ignore`, altrimenti verranno eliminati durante la sincronizzazione.

## Istruzione sync-delay

Istruzione `sync-delay` imposta la lista dei file, durante la modifica dei quali il passaggio del prodotto alla nuova revisione viene bloccato. Il repositorio continua di diffondere la revisione precedente, la sincronizzazione non viene più eseguita (lo stato del prodotto viene "congelato"). Se l'utente considera la revisione ricevuta valida per diffonderla, deve modificare il fil dello stato `.id` e riavviare il **Server** (v. Allegato F3. File .id).

**Esempi:**

- Diffusione automatica di nuove revisioni viene proibita:

```
sync-delay{ .* }
; niente in automatico, tutto da testare
; personalmente
```

- Si proibisce la diffusione automatica delle revisioni, in cui sono aggiornati i file eseguibili:

```
sync-delay{ .*\.exe$ .*\.dll$ }
```

## *Istruzioni state-only e state-ignore*

Istruzioni `state-only` e `state-ignore` nello stesso modo impostano (limitano) la lista dei file da diffondere.

**Esempio:**

Per il prodotto **Enterprise Agent**:

- non si richiede di ottenere la lingua tedesca, polacca e spagnola di interfaccia (altri sono da ricevere),
- non si richiede di ottenere i componenti, destinati per i SO Windows 98/SO Windows Me.

```
sync-ignore{
      ; da notare, se i file elencati sono già
presenti
    ; nel repositorio, sono sempre da diffondere.
    ; quindi si devono eliminare da lì o
    ; elencare in state-ignore{ }, o eseguire
    ; una sincronizzazione completa in questa
    ; configurazione
;^common/ru-.*\.dwl$ questo ci serve
^common/de-.*\.dwl$
^common/pl-.*\.dwl$
^common/es-.*\.dwl$
^win/de-.*
^win/pl-.*
^win-9x\.*
}
```

## *Istruzioni del gruppo notify*

Le istruzioni del gruppo `notify` permettono di configurare il sistema di avvisi per i singoli prodotti (configurazione del sistema di avvisi in generale è descritta in Configurazione avvisi).

Il repositorio può generare i seguenti tipi di avvisi:

- `update` — prodotto è aggiornato con successo,
- `delay` — transazione viene congelata,
- `flushfail` — errore di scrittura sul disco,
- `loadfail` — errore di caricamento.

Di default tutti i tipi di avvisi sono consentiti.

Istruzione `notify-off` permette di proibire tipi concreti di avvisi per tale prodotto.

Istruzioni `notify-ignore` e `notify-only` permettono di limitare o esplicitamente impostare la lista dei file, durante la modifica dei quali viene inviato un avviso del tipo `update`.



Se nel file contemporaneamente sono presenti almeno due delle istruzioni `sync-only`, `sync-ignore` o `sync-delay`, viene utilizzata la regola seguente:

- prima si applica `sync-only`. I file, non elencati nella lista di questa istruzione (se è presente), non vengono elaborati,
- ai file rimanenti viene applicata `sync-ignore`,
- solamente ai file, che rimangono dopo le due voci precedenti, viene applicata `sync-delay`.

Nello stesso modo e ordine si applicano `state-only` e `state-ignore`.

# F3. File .id

*File di stato del prodott* — è un file di testo, dove **Server** registra i numeri delle revisioni del prodotto. Nello stato normale il file contiene un solo numero (numero attuale della revisione). Sincronizzazione del prodotto viene eseguita solo se il numero di revisione sul server **SAM** supera numero attuale, e viene eseguita in quattro fasi:

1. In file `.id` si scrivono 2 numeri:

   *<nuova_revisione>* *<revisione_precedente>*.

   In questo modo si marca che il prodotto sta nella transazione non completata da

   *<revisione_precedente>* a *<nuova_revisione>*.

2. Per HTTP si ottengono tutti i file modificati e si mettono nelle sottocartelle corrispondenti con i nomi del tipo

   *<nome file originale>*`.`*<nuova_revisione>*.

3. Nel file `.id` si scrive il risultato di transazione.

   Può essere lo stato normale, ma già con un nuovo numero, o lo stato "congellato" (`frozen`) se si scatta la regola `sync-delay`:

   *<nuova_revisione>* *<vecchia_revisione>* `frozen`.

4. Se lo stato non è "congellato", i nuovi file sostituiscono i file originali.

Al riavvio del **Server** dopo l'analisi del file `.id` la transazione non completata viene "annullata"; nel caso contrario, viene eseguita la voce **4**.

# F4. Esempi gestione repositorio con modifica del file di stato

***Sincronizzazione completa del prodotto:***

1. Arrestare **Server**.
2. Eliminare tutti i contenuti della cartella del prodotto, oltre `.id` e `.config`.
3. Scrivere `0` nel file `.id`.
4. Avviare il **Server**.
5. Eseguire aggiornamento del prodotto.



Revisione `0` ha il valore speciale, siccome con essa si proibisce diffusione, per questo lo stato "vuoto" del prodotto non viene replicato su **Agent**.

***Divieto di diffusione:***

1. Arrestare **Server**.
2. Scrivere `0` nel file `.id`.
3. Passare ai commenti l'istruzione `sync-with` nel file `.config` per proibire la sincronizzazione.
4. Avviare il **Server**.
5. Eseguire aggiornamento del prodotto.

***Passaggio dallo stato "congellato" alla nuova versione:***

1. Sostituire i contenuti di `.id` di

   *<nuova_revisione>* *<revisione_precedente>* `frozen`

   con

   *<nuova_revisione>*.
2. Riavviare il **Server**.
3. Eseguire aggiornamento del prodotto.

***Tornare dallo stato "congellato" alla versione precedente:***

1. Sostituire i contenuti di `.id` di

   *<nuova_revisione> <revisione_precedente>* `frozen`

   con

   *<nuova_revisione> <revisione_precedente>*.

2. Riavviare il **Server**.
3. Eseguire aggiornamento del prodotto.



Durante i tentativi successivi di sincronizzazione alla *<nuova revisione>*, il repositorio di nuovo passa allo stato "congelato". Salvataggio di *<versione precedente>* del repositorio con rifiuto agli aggiornamenti potrebbe essere giustificato se c'è una revisione conveniente, per esempio, una che abbia già passato con successo il banco di prova.

# Allegato G. File di configurazione

In questa sezione si descrive il formato dei seguenti file:

- file di configurazione di **Enterprise Server** `drwcsd.conf`;
- file di configurazione del **Server proxy** `drwcsd-proxy.xml`;
- file di configurazione del **Centro gestione** `webmin.conf`;
- file di configurazione `download.conf`.



Se sul computer con il componente corrispondente è installato **Agent** con auto-protezione attivata, prima di modifica di file di configurazione si deve disattivare il componente di autoprotezione **Dr.Web SelfPROtect** via le configuazioni di **Agent**.

Salvate tutte le modifiche apportate, si consiglia di attivare il componente **Dr.Web SelfPROtect**.

## G1. File di configurazione di Dr.Web Enterprise Server

File di configurazione di **Enterprise Server** `drwcsd.conf` di default si trova nella sottocartella `etc` della cartella radice del **Server**. Durante l'avvio del **Server** con il parametro di riga di comando si può impostare la location non standard e il nome del file di configurazione (per più informazioni v. Allegato H5. Dr.Web Enterprise Server).

***Se è necessario modificare manualmente il file di configurazione di Dr.Web Enterprise Server, eseguire le seguenti azioni:***

1. Arrestare il **Server** (v. Avvio e arresto di Dr.Web Enterprise Server).
2. Disattivare autoprotezione (se sul computer è presente un **Agent** con autoprotezione attiva - nel menu contestuale di **Agent**).

3. Introdurre modifiche necessarie nel file di configurazione del **Server**.
4. Avviare il **Server** (v. Avvio e arresto di Dr.Web Enterprise Server).

## *Formato dei file di configurazione di Dr.Web Enterprise Server*

Durante la descrizione del file di configurazione del **Server** si utilizza grammatica formale, che si basa sulla notazione EBNF e comprende le seguenti simboli:

- `(...)` — gruppo dei simboli (frammento del file di configurazione),
- `'...'` — simbolo terminale;
- `<...>` — simbolo nonterminale;
- `|` – simbolo di scelta di uno di elementi proposti;
- `(...)?` – simbolo (o gruppo di simboli tra parentesi) a sinistra di operatore non è obbligatorio (può essere ripetuto 0 o 1 volta);
- `(...)*` – simbolo (o gruppo di simboli tra parentesi) a sinistra di operatore può essere ripetuto qualsiasi numero di volte (nonché può essere omesso);
- `(...)+` – simbolo (o gruppo di simboli tra parentesi) a sinistra di operatore può essere ripetuto 1 o più volte;
- `[...]` – qualsiasi simbolo, che rientra nel range indicato;
- punto alla fine — simbolo speciale, che indica che la regola è completata.

**Formato di file di configurazione del Server:**

```
<istruzione> := (<parametro> '"'<valore>'"')? (';'<commento>)?.
<parametro> := <parola>.
<valore> := (<parola> <separatore>*)*.
<parola> := ([a-zA-Z] | [0-9] | <simbolo_speciale>)+.
```

```
<simbolo_speciale> := '&&' | '&r' | '&t' | '&n' | '&v' | '&f'
| '&b' | '&e' | '&l' | '&s'.
<separatore> := \s | \t | \r | \n | \f.
```

Il file di configurazione ha il formato di testo. Elemento di struttura principale del file sono le parole, tra cui possono esserci degli separatori — spazi (`\s`), simboli di tabulazione (`\t`), ritorno del carrello (`\r`), fine linea (`\n`), cambio formato (`\f`). Oltre questo come parola viene considerata una conseguenza dei simboli tra doppie apici `"..."`.

Possono far parte di una parola, non interrompendolo, conseguenze speciali di due simboli, che iniziano con ampersand (&). Sono interpretati in questo modo:

- `&&` — stesso simbolo `&`,
- `&r` — simbolo di ritorno del carrello,
- `&t` — tabulazione,
- `&n` — simbolo di nuova linea,
- `&v` — tabulazione verticale,
- `&f` — cambio formato,
- `&b` — ritorno di un passo,
- `&e` — segno di uguaglianza (`=`),
- `&l` — barra verticale (`|`),
- `&s` — spazio.

Ampersand (`&`), che è ultimo nella linea, — stesso di `&n`.



In questo modo, lo standard ampersand (non utilizzato ai fini di creazione di una conseguenza speciale) deve essere doppiato.

I commenti iniziano con punto e virgola e durano fino a fine linea.

Le configurazioni del **Server** si impostano nel file di configurazione nel formato di istruzioni, ognuna delle quale rappresenta un parametro, che consiste di una parola, dopo di cui possono seguire i suoi valori (una o più parole).

Di seguito sono descritte possibili istruzioni. L'ordine di conseguenza di istruzioni nel file non è importante. Nelle parentesi quadre - valori dei parametri, impostati dall'utente.

- `Name` *<nome>*

  Definisce la denominazione (il nome) del **Server**, a cui risponderà alla ricerca del **Server** da **Agent** o **Cento gestione**. Valore predefinito — riga vuota ("") significa utilizzo del nome di computer.

- `Threads` *<numero>*

  Numero dei thread del **Server**, che servono i client. Predefinito — 5. Non si deve modificare il valore del parametro senza il consiglio del supporto.

- `DBPool` *<numero>*

  Numero di connessioni del database al **Server**. Per i **Server** del SO Windows e **Server** del SO UNIX - di default è 2. Non si deve modificare il valore del parametro senza il consiglio del supporto.

- `MaximumAuthorizationQueue` *<numero>*

  Imposta quantità massima di workstation in fila per autorizzazione sul **Server**. Non si deve modificare il valore del parametro senza il consiglio del supporto.

- `Newbie` *<modalità>*

  Modalità di accesso di workstation nuove, può avere valori `Open`, `Close` o `Approval` (predefinito `Approval`). Per più informazioni v. Politica di connessione di workstation nuove.

- `UnAuthorizedToNewbie` *<modalità>*

  Modalità può avere valori o `Yes` — che significa che workstation che non hanno passato autorizzazione (per esempio, nel caso di guasto del database), saranno automaticamente passate allo

stato di nuove, o `No` (predefinito), che significa modalità standard di operazione.

- `WEBStatistics "Interval=`*<numero>*
  `Server=`*<indirizzo_server>*
  `URL=`*<cartella>*
  `ID=`*<identificatore_client>*
  `User=`*<utente>*
  `Password=`*<password>*
  `Proxy=`*<server_proxy>*
  `ProxyUser=`*<utente_proxy>*
  `ProxyPassword=`*<password_proxy>*`"`

  Viene descritto il server web, su cui **Enterprise Server** pubblicherà le sue statistiche sui virus rilevati.

  Intervallo di pubblicazione viene impostato in minuti, di default è 30.

  Indirizzo del server predefinito `stat.drweb.com:80`

  `URL` di default `/update`.

  `ID` — identificatore del client (di default calcolato da chiave del server di utente `enterprise.key`).

  Campi `User` e `Password` descrivono autorizzazione sul server web, il resto - server proxy e autorizzazione su di esso. Di default i campi sono vuoti (autorizzazione non è richiesta).

  Per ottenere accesso alla informazione, conservata sul server di statistiche, rivolgersi al supporto.

- `Encryption` *<modalità>*

  Modalità di codifica del traffico. Valori consentiti: `Yes`, `No`, `Possible` (di default `Yes`). Per più informazioni v. Utilizzo di codifica e compressione del traffico.

- `Compression` *<modalità>*

Modalità di compressione del traffico. Valori consentiti: `Yes`, `No`, `Possible` (di default `No`). Per più informazioni v. Utilizzo di codifica e compressione del traffico.

- `InstallAccess`, `AgentAccess` e `LinksAccess` non si visualizzano nel file di configurazione, se il flag **Utilizzare questa lista di accesso** non è posto (v. Configurazione di Dr.Web Enterprise Server). Se il flag è posto, i valori visualizzati di parametri disattivati sono "`none`". Per parametri connessi saranno visualizzati indirizzi impostati.
- `Database` *<DRIVER>* `from` *<PATH>* `using` *<PARAMETERS>*

  Definizione del database. *<DRIVER>* — nome di driver del database, *<PATH>* — percorso, dove caricare il driver, *<PARAMETERS>* — parametri di stabilimento di connessione con il server del database. Per più informazioni v. Configurazione di modalità di operazione con il database.



Questa istruzione può essere utilizzata nel file di configurazione una volta sola.

- `Alert` *<DRIVER>* `from` *<PATH>* `using` *<PARAMETERS>*

  Definizione del programma di avvisi. *<DRIVER>* — nome di driver del programma di avvisi, *<PATH>* — percorso, da dove scaricare driver, *<PARAMETERS>* — parametri del programma di avvisi. Per più informazioni v. Configurazione avvisi.



Questa istruzione può essere utilizzata nel file di configurazione una volta sola.

In questa e successiva istruzioni i parametri nel campo `using` si separano da spazi. Il nome del parametro viene separato dal valore dal segno di uguaglianza `(=)`, che non deve essere circondato da spazi. Se il parametro può avere più di un valore, si separano uno dall'altro da barra verticale `(|)`. Se nel valore del parametro c'è il segno di

uguaglianza, barra verticale o spazio si sostituiscono di conseguenza con `&&e`, `&&l`, `&&s` rispettivamente.

- `transport` *<NAME> <STREAM> <DATAGRAM>*

  Definizione dei protocolli di trasporto e il loro linking alle interfacce di rete. *<NAME>* — nome del **Server**, impostato come in istruzione `name` (v. sopra), se è impostata una riga vuota, viene preso dal `name`. *<STREAM>* (per esempio, `tcp/`), *<DATAGRAM>* (per esempio, `udp/`) hanno il formato, descritto in Allegato E. Specifica di indirizzo di rete

- `Disable Message` *<avviso>*

  Bloccare invio di avvisi di un certo tipo, valori ammissibili del parametro - tipo di messaggio, per la lista completa di tutti i tipi dei messaggi v. la cartella `templates`.

- `Disable Protocol` *<protocollo>*

  Bloccare utilizzo di uno dei protocolli del server, valori ammissibili: `AGENT`, `SERVER`, `INSTALL`, `CONSOLE`. Nel file di configurazione di default è presente una instruzione che blocca il protocollo `SERVER`. Per più informazioni v. Configurazione di Dr.Web Enterprise Server.

  Blocco dei protocolli che non servono risparmia le risorse del sistema.

- `Disable Plugin` *<valore>*

  Bloccare utilizzo di plugin supplementari del **Server**, valore ammissibile: `WEBMIN`. Per più informazioni v. Configurazione di Dr.Web Enterprise Server.

- `ShowHostNames` *<valore>*

  Consentire di visualizzare nel log i nomi di dominio dei computer invece di indirizzo TCP. Valori possibili: `Yes` o `No`.

- `ReplaceNetBIOSNames` *<valore>*

Consentire di sostituire nomi NetBIOS dei computer con il nome DNS. Valori possibili: `Yes` o `No`.

- Parametri `Società`, `Reparto`, `Paese`, `Regione`, `Città`, `Via`, `Piano`, `Stanza`, `Latitudine` e `Longitudine` impostano le informazioni supplementari su location geografica e corporativa di workstation.
- `TrackAgentJobs` *<valore>*

  Consentire di scrivere nel dabase il risultato di esecuzione dei processi su workstation. Valori possibili: `Yes` o `No`.

- `TrackAgentStatus` *<valore>*

  Consentire di registrare le modifiche dello stato di workstation e di scrivere le informazioni nel database. Valori possibili: `Yes` o `No`.

- `TrackVirusBases` *<valore>*

  Consentire di registrare lo stato (composizione, modifiche) di database dei virus su workstation e di scrivere le informazioni nel database. Valori possibili: `Yes` o `No`.

- `TrackAgentModules` *<valore>*

  Consentire di scrivere nel database le informazioni su tutti i plugin di **Dr.Web** anti-virus, installati su workstation. Valori possibili: `Yes` o `No`.

- `TrackAgentComponents` *<valore>*

  Consentire di scrivere nel database le informazioni su tutti i componenti antivirus, installati su workstation. Valori possibili: `Yes` o `No`.

- `KeepRunInformation` *<valore>*

  Consentire di scrivere nel database le informazioni su avvio e completamenti di operazione dei componenti di **Antivirus (Scanner**, **Monitor** ecc) su workstation. Valori possibili: `Yes` o `No`.

- `KeepInfections` *<valore>*

Consentire di scrivere nel database i dati statistici sulle infezioni, rilevate su workstation. Valori possibili: `Yes` o `No`.

- `KeepScanErrors` *<valore>*

  Consentire di scrivere nel database le informazioni su tutti gli errori durante la scansione su workstation. Valori possibili: `Yes` o `No`.

- `KeepScanStatistics` *<valore>*

  Consentire di scrivere nel database i risultati di scansione su workstation. Valori possibili: `Yes` o `No`.

- `KeepInstallation` *<valore>*

  Consentire di scrivere nel database le informazioni su installazioni di **Agent** su workstation. Valori possibili: `Yes` o `No`.

- `Quarantine` *<valore>*

  Consentire di scrivere lo stato di **Quarantena** su workstation. Valori possibili: `Yes` o `No`.

- `UpdatesBandwidth` *<valore>*

  Larghezza massima di banda di trasmissione del traffico di rete in kB durante la trasmissione di aggiornamenti tra **Server** e **Agent**. Valore `0` - banda di trasmissione non è limitata.

- `Audit` *<valore>*

  Consentire di gestire il log di audit delle operazioni dell'amministratore con il **Centro gestione** e la scrittura del log nel database. Valori possibili: `Yes` o `No`.

- `AuditInternals` *<valore>*

  Consentire di gestire il log di audit delle operazioni interne del **Server** e la scrittura del log nel database. Valori possibili: `Yes` o `No`.

# G2. File di configurazione del Centro gestione di Dr.Web

Il file di configurazione del **Centro gestione** `webmin.conf` si trova nella sottocartella `etc` della cartella radice del **Server**.

Durante la descrizione del file di configurazione del **Centro gestione** si utilizza grammatica formale, che si basa sulla notazione EBNF e comprende i seguenti simboli:

- `(...)` — gruppo dei simboli (frammento del file di configurazione),
- `'...'` — simbolo terminale;
- `<...>` — simbolo nonterminale;
- `|` – simbolo di scelta di uno di elementi proposti;
- `(...)?` – simbolo (o gruppo di simboli tra parentesi) a sinistra di operatore non è obbligatorio (può essere ripetuto 0 o 1 volta);
- `(...)*` – simbolo (o gruppo di simboli tra parentesi) a sinistra di operatore può essere ripetuto qualsiasi numero di volte (nonché può essere omesso);
- `(...)+` – simbolo (o gruppo di simboli tra parentesi) a sinistra di operatore può essere ripetuto 1 o più volte;
- `[...]` – qualsiasi simbolo, che rientra nel range indicato;
- punto alla fine – simbolo speciale, che indica che la regola è completata.

***Formato del file di configurazione del Centro gestione Dr.Web:***

```
<istruzione> := <parametro>* (';'<commento>)?.

<parametro> := <singolare> | <blocco>.
<singolare> := <nome> <nome>.
<gruppo> := <nome> '{' (<valore>' ')+ '}'.
<blocco> := <prefisso>? <nome> '{' <singolare>* | <gruppo>* |
```

```
<accesso>? | <autorizzazione>? '}'.

<prefisso> := 'Static' | 'Handler' | 'Scripts' | 'Mixed'.
<accesso> := 'Access {'
             'Secure {'
                'Priority ' <priorità>?
                ('Allow {' <valore>* '}')?
                ('Deny {' <valore>* '}')?
             '}'
             'InSecure {'
                'Priority ' <priorità>?
                ('Allow {' <valore>* '}')?
                ('Deny {' <valore>* '}')?
             '}'
          '}'.
<priorità> := 'deny' | 'allow'.

<autorizzazione>:= 'Authorization {' <singolare>+ | <gruppo>+ '}'.

<nome> := <parola>.
<valore> := <nome> <separatore>*.
<parola> := ( [a-zA-Z] | [0-9] | <segno> )+.
<separatore> := \s | \t | \r | \n | \f.
<segno> := '/' | '*' | ':' | '.' | '-' | '?' | '^'| '[' |
']'.
```

Il file di configurazione ha il formato di testo. Elemento di struttura principale del file sono le parole, tra cui possono esserci degli separatori — spazi (`\s`), simboli di tabulazione (`\t`), ritorno del carrello (`\r`), fine linea (`\n`), cambio formato (`\f`).

I commenti iniziano con punto e virgola e durano fino a fine di linea.

Le configurazioni del **Centro gestione** si impostano nel file di configurazione come istruzioni, ognuna delle quali rappresenta:

- parametro, che consiste di una parola (nome del parametro),

dopo di cui segue il suo valore (una o più parole),

- blocco dei parametri, che consiste di una parola (nome del blocco), dopo di cui tra parentesi graffe possono essere definiti:
  - parametri semplici, che rappresentano una parola (nome del parametro), dopo di cui segue il valore (uno o più parole),
  - gruppi dei parametri, che rappresentano una parola (nome del parametro), dopo di cui tra parentesi graffe segue il set dei valori (uno o più parole),
  - gruppo dei parametri `Access`, che definisce regole di accesso alle risorse impostate del server (v. sotto),
  - gruppo dei parametri `Authorization`, che definisce i parametri di autorizzazione per accesso alle risorse impostate (v. sotto).

Prima del nome del blocco dei parametri può essere impostato un prefisso - una parola, che definisce il principio di elaborazione dei parametri del blocco.

Sotto sono descritte alcune delle istruzioni disponibili. L'ordine di conseguenza di istruzioni nel file non è importante.

Maggior parte dei parametri semplici (singolari) sono impostati con valori predefiniti e non richiedono modifiche. Ma durante operazione del **Server** può essere richiesta impostazione dei valori per alcuni di essi:

- `ServerName` *<DNS_nome>*:*<numero_porta>* – definisce il nome del **Server** e la porta. Si utilizza per sostituzione nelle richieste durante il richiamo del **Server**. Si devono inserire i valori corrispondenti subito dopo l'installazione del **Server** (v. Installazione di Dr.Web Enterprise Server).
- `Listen` *<protocollo>* *<interfaccia>*:*<numero_porta>* – imposta i parametri di interfacce ascoltate. Utilizzato per configurare accesso al **Centro gestione**.

I blocchi di parametri contengono i seguenti gruppi e parametri:

- Prefisso (`Static`, `Script`, `Handler` o `Mixed`) viene impostato prima del nome del blocco dei parametri e definisce il principio di elaborazione di richieste di utente corrispondenti.

- Prefisso `Static` definisce il metodo di elaborazione statistico, che prevede trasmissione all'utente del valore finito - del file richiesto senza modifiche (per esempio, di immagine, conservato sul **Server**).

- Prefisso `Handler` definisce metodo di elaborazione, che prevede esecuzione di script, impostato nei parametri del blocco, al ricevimento di richiesta dell'utente (correttezza dei percorsi, indicati nella richiesta, non è importante). In questo caso nel corpo successivo del blocco di istruzioni deve essere presente l'istruzione `Script` *<nome_di_script>*, che definisce lo script eseguito.

- Prefisso `Scripts` definisce il metodo di elaborazione di richieste, che prevede esecuzione di tutti i file dalla richiesta di utente come script.

- Prefisso `Mixed` imposta metodo di elaborazione misto, che prevede unione di due metodi - `Static` e `Scripts`. In questo caso nel corpo successivo del blocco di istruzioni deve essere presente il gruppo dei parametri `Scripts { `*<estensioni_di_script>*` }`, che definisce script eseguibili (per estensione). Tutti gli altri file, che non corrispondono ai valori di questo gruppo dei parametri, saranno passati statisticamente (così come sono, senza elaborazione).

◆ Gruppo dei parametri `Access` contiene la definizione dei diritti di accesso alle risorse del **Server** durante elaborazione di richieste dell'utente ricevute.

- Gruppo `Secure` imposta i diritti di accesso per connessioni protette per protocollo HTTPS.

- Gruppo `InSecure` imposta i diritti di accesso per connessioni non protette per protocollo HTTP.

- Parametro `Priority` *<priorità>* definisce priorità di elaborazione delle liste di connessioni consentite e bloccate. Quando si imposta il valore `deny`, tutti gli indirizzi, che non non fanno parte di tutti e due gruppi (`Allow` e `Deny`), saranno bloccati, se si imposta il valore `allow` - saranno consentiti.
- La lista dei parametri del gruppo `Allow` imposta indirizzi di nodi, la accesso dai quali al **Server** sarà consentito.
- La lista dei parametri del gruppo `Deny` imposta indirizzi di nodi, la accesso dai quali al **Server** sarà bloccato.

Indirizzi nelle liste di nodi bloccati/consentiti si impostano nel formato:

per TCP/IP: `tcp/`*<indirizzo_IP>*`[/`*<prefisso>*`]`;

per SPX: `spx/`*<numero_rete>*`[.`*<indirizzo_workstation>*`]`.

- Gruppo dei parametri `Authorization` definisce parametri necessari di autorizzazione dell'utente durante il richiamo del **Server** per elaborare la richiesta corrispondente.

## G3. File di configurazione download.conf

***Scopo del file download.conf:***

1. Se viene creato e usato un sistema di cluster dei **Enterprise Server**, consente di distribuire il carico tra i **Server** dei cluster se si connettono un grande numero di workstation nuove.
2. Se sul **Enterprise Server** si usa una porta personalizzata, consente di impostare questa porta quando si genera il file di installazione di **Agent**.

Il file `download.conf` si usa quando si genera il file di installazione di **Agent** per una nuova postazione della rete antivirus. I parametri di questo file consentono di impostare l'indirizzo di **Enterprise Server** e la porta che vengono utilizzati per connettere il programma di installazione di **Agent** al **Server** in formato:

```
download = { server = '<Server_Address>'; port =
```

```
<port_number> }
```

dove:

- *<Server_Address>* - l'indirizzo IP o il nome DNS del **Server**.

  Quando si genera il pacchetto di installazione di **Agent**, l'indirizzo di **Server** inizialmente viene preso dal file `download.conf`. Se nel file `download.conf` non è impostato l'indirizzo di **Server**, viene utilizzato il valore del parametro `ServerName` dal file `webmin.conf`. Altrimenti si usa il nome del computer restituito dal sistema operativo.

- *<port_number>* - la porta per connettere il programma di installazione di **Agent** a **Server**.

  Se la porta non è indicata nei parametri del file `download.conf`, di default viene usata la porta 2193 (si configura in **Centro gestione** nella sezione **Amministrazione → Configurazione Dr.Web Enterprise Server →** scheda **Trasporto**).

Di default il parametro `download` nel file `download.conf` è commentato. Per usare il file `download.conf`, decommentare questo parametro cancellando "`--`" all'inizio della riga e impostare i valori rilevanti dell'indirizzo e della porta di **Server**.

## G4. File di configurazione del server proxy

Il file di configurazione del **Server proxy** `drwcsd-proxy.xml` è in formato XML e si trova:

- Per i SO Windows: nella cartella di installazione del **Server proxy**.
- Per i SO della famiglia UNIX: nella sottocartella `etc` della cartella di installazione del **Server proxy** o nella cartella operativa attuale dell'utente.

## Elemento <cache-root />

Elemento radice <drwcsd-proxy /> può inoltre contenere elemento non obbligatorio <cache-root />, in cui si indica il percorso alla cartella cash del **Server proxy**. Se elemento <cache-root /> non è impostato, i dati messi in cash verranno salvati nella cartella temporanea di utente del SO.

## Elemento <listen />

Elemento radice <drwcsd-proxy /> contiene uno o più elementi obbligatori <listen />, che definiscono le configurazioni principali per ricevere connessioni da **Server proxy**. Elemento <listen /> contiene unico attributo obbligatorio `spec`, le cui proprietà definiscono su quale interfaccia "ascoltare" le connessioni di client in entrata e se si avvia su questa interfaccia modalità `discovery`. Attributo `spec` contiene le seguenti proprietà:

- `protocollo` – tipo di protocollo per ricevere le connessioni in entrata. Come parametro viene indicato l'indirizzo, ascoltato da **Server proxy**.
- `porta` – numero di porta, ascoltata da **Server proxy**.
- `modalità di imitazione` – modalità di imitazione del **Server**. Permette a **Scanner di rete** di rilevare **Server proxy** come **Enterprise Server**.
- `gruppo multicast` – gruppo a più indirizzi, in cui si trova **Server proxy**.

I valori delle proprietà di attributo `spec` e i loro parametri sono riportati in tabella G-1.

**Tabella G-1. Proprietà di elemento spec**

| Proprietà | Obbliga-torio | Valori ammissibili | Parametri di valori ammissibili | |
|---|---|---|---|---|
| | | | consentiti | predefiniti |
| protocollo | sì | ip,<br>ipx,<br>netbios | | 0.0.0.0<br>–<br>– |
| porta | no | port | | 2193 |
| modalità imitazione | no | discovery | sì, no | no |
| gruppo multicast | no | multicast | | 231.0.0.1 |

Attributo `spec` contiene una proprietà obbligatoria – `protocollo` e tre proprietà non obbligatorie: `porta`, `modalità di imitazione` e `gruppo multicast`. A secondo del valore, che ha la proprietà `protocollo`, i contenuti della lista delle proprietà non obbligatorie, indicate in attributo `spec`, si possono cambiare.

Nella tabella G-2 è riportata la lista delle proprietà non obbligatorie, che possono essere impostati (+) o non possono essere impostati (–) in attributo `spec` a secondo il valore del parametro `protocollo`.

**Tabella G-2. Presenza delle proprietà non obbligatorie a secondo del valore del parametro protocollo**

| Protocollo | Presenza delle proprietà | | |
|---|---|---|---|
| | port | discovery | multicast |
| ip | + | + | + |
| ipx | + | + | – |
| netbios | + | + | – |

## *Elemento <forward />*

Le configurazioni, che definiscono reindirizzamento delle connessioni in entrata, vengono impostati da elemento `<forward />`, che è un elemento figlio di elemento `<listen />`. Elemento `<forward />` contiene uno o più attributi obbligatori `to`, come valori delle quali si impostano indirizzi di **Enterprise Server**, su uno delle quali verrà reindirizzata la connessione. Indirizzo di **Enterprise Server** viene impostato a secondo della specifica di indirizzo di rete, in particolare, nel formato `tcp/`*<nome_DNS>*`:`*<porta>*.

Elemento `<forward />` è obbligatorio. In questo caso elemento `<listen />` può contenere più elementi `<forward />`.

### *Algoritmo di reindirizzamento se è disponibile una lista dei Enterprise Server:*

1. Il **Server proxy** carica nella memoria operativa una lista dei **Enterprise Server** dal file di configurazione `drwcsd-proxy.xml`.
2. Il **Enterprise Agent** si connette al **Server proxy**.
3. Il **Server proxy** reindirizza il **Enterprise Agent** al primo **Enterprise Server** dalla lista che si trova nella memoria operativa.
4. Il **Server proxy** ruota la lista caricata nella memoria operativa e sposta il **Enterprise Server** dalla prima voce alla fine della lista.



Il **Server proxy** non memorizza la sequenza modificata dei **Server** nel suo file di configurazione. Al riavvio del **Server proxy**, la lista dei **Enterprise Server** viene caricata nella memoria operativa nella sua versione originale, conservata nel file di configurazione.

5. Quando un altro **Agent** si connette al **Server proxy**, la procedura si ripete dal punto 2.

6. Se il **Enterprise Server** si disconnette dalla rete antivirus (per esempio, in caso di spegnimento o negazione del servizio), l'**Agent** si connette di nuovo al **Server proxy** e la procedura si ripete dal punto 2.

## *Esempio del file di configurazione drwcsd-proxy.xml*

```
<?xml version="1.0"?>
<drwcsd-proxy>
  <!-- Specify path to cahe directory, if not specified wi
  <cache-root>C:\Work\es_head\build\a-x86\bin\var</cache-ro

  <!-- property: ip, ipx, netbios, unx: define protocol fa
  <!-- property: port: define port to listen on. Default 21
  <!-- property: name: define discovery name. Default drwcs
  <!-- property: discovery: define should proxy run discove
  <!-- property: multicast: define should proxy enter to mu

  <!-- For example -->
  <!-- Listen on IN_ADDR_ANY port 2193, run discovery on 21
  <listen spec="ip(), multicast()">
    <!-- one or more forward tags-->
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>

  <!-- Listen on ipv6 IN6_ADDR_ANY, port 2194, run discover
  <listen spec="ip([]), port(2194), multicast()">
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>

  <!-- Listen on default ipx, port 2194, run simple discove
  <listen spec="ipx(), discovery()">
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>

  <!-- Listen on default netbios, port 23, lana 0, run simp
  <listen spec="netbios(), discovery()">
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>
</drwcsd-proxy>
```

# Allegato H. Parametri riga di comando di programmi, che fanno parte di Dr.Web Enterprise Security Suite

## H1. Introduzione

I parametri di riga di comando hanno la priorità più alta delle configurazioni predefiniti o altre configurazioni costanti (impostati nel file di configurazione del **Server**, registro del SO Windows ecc). In alcuni casi i parametri impostati all'avvio inoltre redefiniscono le configurazioni costanti. Questi casi sono descritti sotto.

Una parte dei parametri di riga di comando ha la forma di chiave – inizia con trattino. Tali parametri si chiamano chiavi.

Tante chiavi possono essere rappresentati in vari formi equivalenti. Così le chiavi che comprendono un valore logico (sì/no, consentire/bloccare), hanno la variante negativa, per esempio, la chiave `-admin-rights` ha una coppia `-no-admin-rights` con il valore contrario. Si possono dare con indicazione esplicita del valore, per esempio, `-admin-rights=yes` e `-admin-rights=no`.



I sinonimi di valore `yes` sono i valori `on`, `true`, `OK`. I sinonimi di `no` sono `off`, `false`.

Se il valore della chiave contiene spazi o tabulazione, tutto il parametro è da rinchiudere in virgolette, per esempio:

```
"-home=c:\Program Files\DrWeb Enterprise Suite"
```

Durante la descrizione di sintassi dei parametri di singoli programmi la parte non obbligatoria viene posta fra parentesi quadre `[...]`.

I nomi delle chiavi possono essere abbreviati (lasciando le ultime lettere), se il nome abbreviato non corrisponde a una parte iniziale di un'altra chiave.

## H2. Plugin di interfaccia di Dr.Web Enterprise Agent

Il plugin di interfaccia di **Agent** viene avviato per ogni utente, registrato sul computer nel modo interattivo. Nei computer nei SO Windows NT e superiori opera con i diritti di questo utente. Per operazione di **Agent** si richiede che la shell di utente sia lo standard **Windows Explorer** o altro programma completamente compatibile con esso.

### *Formato di comando di avvio:*

`drwagnui [<chiavi>]`

### *Chiavi consentiti:*

- `-admin-rights` o `-no-admin-rights` — consentire o bloccare modalità amministrativa di operazione nei SO Windows 98/ SO Windows Me (cioè se l'utente, che opera in queste versioni, viene considerato l'amministratore). L'amministatore può, in partioclare, modificare le configurazioni di **Agent**. Nel SO Windows NT e superiori questo viene definito dal sistema dei diritti del SO. Di default si prevede il blocco.
- `-delay=`*<numero>* — fra quanti minuti visualizzare il messaggio di saluto all'utente dopo l'avvio. Tempo predefinito - 2 minuti, valore `-1` permette di disattivare il saluto.
- `-help` — visualizzare la guida ai formati di comando.
- `-trace` — registrare in dettagli dove si è riscontrato un errore, applicabile anche in altre applicazioni.

## H3. Dr.Web Enterprise Agent

Le impostazioni di **Agent** si custodiscono nel registro di Windows nel ramo `HKEY_LOCAL_MACHINE\SOFTWARE\IDAVLab\Enterprise Suite\Dr.Web Enterprise Agent\Settings`, e per i parametri definiti da chiavi, il nome del parametro coincide con il nome della chiave.

La lista dei server **SAM** a cui **Agent** può collegarsi si custodisce nei file `.config` locati nelle sottocartelle del repository (per SO Windows - `DrWeb Enterprise Server\var\repository\`).

Se **Agent** viene avviato con alcuni parametri esplicitamente indicati, queste impostazioni non solo vengono usate nella sessione corrente, ma anche vengono trascritti nel registro e diventano impostazioni permanenti. Così, se si è avviato una volta **Enterprise Agent** con tutti i parametri necessari, non si dovrà impostare i parametri di nuovo agli avvii successivi.



Le impostazioni di **Agent** definite direttamente sulla workstation vengono sovrascritte dalle impostazioni ricevute da **Server**.

Se su **Server** viene impostata una lista vuota di **Server** a cui si connette la workstation, sarà utilizzata la lista di **Server** impostata sulla workstation.

**Enterprise Agent** viene avviato dal sistema come servizio e viene gestito tramite il **Pannello di controllo**.

***Formato del comando avvio:***

`drwagntd [<chiavi>] [<server>]`

## Chiavi

### Chiavi ammissibili:

- `-compression=<modalità>` — la modalità di compressione del traffico verso e da **Server**. I valori ammissibili sono `yes`, `no`, `possible` (di default `possible`).
- `-control=<azione>` — gestisce lo stato del servizio di **Agent**. Le azioni ammissibili sono:
  - `install` — installare il servizio,
  - `uninstall` — eliminare il servizio,
  - `start` — avviare il servizio (solo in SO Windows NT e superiore),
  - `stop` — arrestare il servizio (solo in SO Windows NT e superiore),
  - `restart` — riavviare il servizio (solo in SO Windows NT e superiore).
- `-crypt=<modalità>` — la modalità di codifica del traffico verso e da **Server**. I valori ammissibili sono `yes`, `no`, `possible` (di default `yes`).
- `-drweb-key=<chiave_licenza>` — la chiave di licenza di utente. Questa chiave verrà usata dal software client se non ci sia la connessione a **Server** per un lungo tempo e se sia scaduta la chiave ricevuta da **Server**. Se la connessione a **Server** è disponibile, questa chiave non è richiesta. Di default è una chiave valida che si trova nella cartella impostata dal parametro `-home`.
- `-help` — visualizzare la guida al formato del comando e ai suoi parametri. È simile a `-help` del plugin di interfaccia, vedi l'Allegato H2. Plugin di interfaccia di Agent Dr.Web Enterprise Agent.
- `-home=<cartella>` — la cartella in cui è installato **Agent.** Se la chiave non è impostata, si intende la cartella in cui si trova il file eseguibile di **Agent**.
- `-key=<chiave_server_aperta>` — il file della chiave aperta di **Server**, di default è `drwcsd.pub` che si trova nella cartella

impostata da `-home`.

- `-log=`*<file_log>* — il file di log del funzionamento di **Agent**, di default viene messo nella sottocartella `logs` della cartella di installazione di **Agent**. Per custodire il file di log dell'eliminazione di **Agent** si usa la cartella di sistema per file temporanei.
- `-retry=`*<numero>* — il numero di tentativi di cercare **Server** tramite l'invio di query multicast (se si usa la ricerca) prima che venga visualizzato il messaggio di fallimento. Di default è **3**.
- `-rotate=`*<N><f>*,*<M><u>* — modalità di rotazione del log del funzionamento di **Agent**, dove:
  - *<N>* — il numero totale di file di log (compresi il file attuale e quelli di archivio);
  - *<f>* — il formato di memorizzazione dei file di log, i valori ammissibili sono `z` (gzip) - comprimere file, si usa di default, oppure `p` (plain) - non comprimere file.
  - *<M>* — dimensione del file;
  - *<u>* — unità di misura, i valori ammissibili sono `k` (kilo), `m` (mega), `g` (giga).

  Di default è `10,10m`, che significa: "custodire 10 file di 10 megabyte, comprimere file". Si può inoltre usare il formato speciale `none (-rotate=none)` che significa: "non usare la rotazione e registrare informazioni sempre nello stesso file di una dimensione illimitata".

  Se si usa la modalità di rotazione, si usa il seguente formato dei nomi di file: `file.`*<N>*`.log` oppure `file.`*<N>*`.log.dz`, dove *<N>* è il numero d'ordine: 1, 2 ecc.

  Per esempio, se il nome del file di log (v. la sopraindicata chiave `-log`) è stato impostato come `file.log`, allora:

  - `file.log` — è il file attuale (in cui si registrano le informazioni),
  - `file.1.log` — è il file precedente,
  - `file.2.log` e così via — il maggiore è il numero, la più vecchia è la versione del file di log.
- `-save` *<indirizzo-IP>* — verifica la correttezza del valore

dell'indirizzo IP di **Server** e memorizza impostazioni nel registro.

- `-spiderstat=<intervallo>` — l'intervallo in minuti per spedire a **Server** informazioni statistiche di **SpIDer Guard**, di default è **30**. Le informazioni statistiche verranno spedite a **Server** fra tali intervalli sempre che in questo tempo siano cambiate.
- `-timeout=<tempo>` — il limite di tempo in secondi per aspettare ciascuna risposta durante la ricerca di **Server**. Messaggi di risposta si ricevono finché il tempo per aspettare risposta non sia esaurito (non supera il valore di timeout). Di default è **5**.
- `-trace` — registrare informazioni di log dettagliate nel posto, dove è accaduto l'errore; si può usare anche in altre applicazioni.
- `-verbosity=<livello_dettagli>` — il livello di dettagli del log. Di default è `INFO`. I valori ammissibili sono: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. I valori `ALL` e `DEBUG3` sono sinonimi (v. anche Allegato L. Formato dei file del log).



Questa chiave determina il grado di dettagli da registrare nel file di log che si imposta dalla chiave `-log` (vedi sopra) che segue questa chiave. Lo stesso comando può includere più chiavi di questo tipo.

Le chiavi `-verbosity` e `-log` dipendono da posizione.

Se queste chiavi si usano contemporaneamente, la chiave `-verbosity` deve stare prima della chiave `-log`, perché la chiave `-verbosity` ridefinisce il livello di dettagli dei log che si trovano ai percorsi impostati più avanti nella riga di comando.

## *Server*

*<server>* — la lista dei **Server**. Di default è `drwcs@udp/231.0.0.1:2193` che significa: "cercare **Server** `drwcs` utilizzando query multicast per il gruppo `231.0.0.1` per la porta `2193`".

# H4. Installazione di rete

***Formato di comando di avvio:***

`drwinst [<chiavi>] [<variabili>] [<server>]`

## *Chiavi*

***Chiavi ammissibili:***

- `-compression=<modalità>` — modalità di compressione del traffico con il **Server**. Valori ammissibili `yes`, `no`, `possible` (predefinito `no`).
- `-help` — visualizzare la guida. Simile al plugin di interfaccia di **Agent**.
- `-home=<cartella>` — cartella di installazione. Predefinita – `"Program Files\DrWeb Enterprise Suite"` sul disco di sistema.
- `-id=<identificatore_workstation>` — imposta identificatore di workstation, su cui viene installato **Agent**.
- `-interactive` — avviare installazione in modalità interattiva.

  La descrizione di installazione di **Agent** in modalità interattiva (grafica) di installazione è riportata nella sezione Installazione di Dr.Web Enterprise Agent.

  Se la chiave `-interactive` non è impostata, installazione di **Agent** verrà eseguita nella modalità background del programma di installazione (v. sezione Installazione di Dr.Web Enterprise Agent). In questo caso l'interfaccia grafica interattiva di installazione può essere visualizzata se c'è un errore di installazione o errore di avvio di installazione.

---



Durante installazione remota di **Agent** con utilizzo del **Centro gestione** questa chiave non funziona.

Chiave `-interactive` non può essere utilizzato insieme ai variabili. Se si impostano i variabili, saranno ignorati.

- `-key=`*<chiave_aperta>* — percorso completo al file della chiave aperta del **Server**. Di default la chiave `drwcsd.pub` si trova nella sottocartella `Installer` della cartella di installazione del **Server**.
- `-log=`*<file_del_log>* — percorso completo al file del log di installazione (indicata durante installazione di **Agent**) o eliminazione (indicata nel caso di disinstallazione di **Agent**).

  Per salvare il file del log di installazione di default si utilizza la sottocartella `logs` della cartella, impostata nella chiave `-home` durante installazione.

  Per salvare il file del log di eliminazione di default si utilizza la cartella dell'utente dei file temporanei.



Se la chiave `-log` non è indicata, i nomi dei file del log vengono generati automaticamente con utilizzo di GUID e di nome del computer.

- `-platforms=p1,p2,p3...` — ordine di caricamento di piattaforme (di default è standard, v. Allegato J. Utilizzo di script di installazione iniziale per Dr.Web Enterprise Agent).
- `-pwd=`*<password>* — inserire password di **Agent** per accedere al **Server**.
- `-regagent` — registrare **Agent** nella lista **Installazione e eliminazione programmi** (**Add or Remove Programs**).
- `-retry=`*<numero>* — analogo ad **Agent**.
- `-script=`*<nome_script>* — imposta il file con lo script eseguibile. Utilizzato insieme alla chiave `-uninstall` per disinstallare software antivirus.
- `-timeout=`*<ora>* — analogo ad **Agent**.
- `-trace` — eseguire il logging dettagliato di dove è successo un errore, applicabile anche in altri applicazioni.
- `-uninstall` — disinstallazione del pacchetto da workstation,

eseguendo lo script di disinstallazione (v. chiave `-script`). Se lo script non è indicato esplicitamente, verrà eseguito lo script interno di disinstallazione.

Se questa chiave non c'è (uguale all'impostazione `-no-uninstall`) viene eseguita installazione.

- `-verbosity=`*<livello_dettagli>* — livello di dettagli del log (analogo ad **Agent**, v. H3. Dr.Web Enterprise Agent). Di default `ALL`.



Questa chiave definisce il livello di dettagli di logging nel file, impostato da chiave che segue dopo `-log` (v. sopra). In questo comando possono esserci più chiavi di questo tipo.

Chiavi `-verbosity` e `-log` dipendono da posizione.

Se queste chiavi si utilizzano contemporaneamente, la chiave `-verbosity` deve precedere la chiave `-log`: la chiave `-verbosity` redefinisce il livello di dettagli dei log, locati ai percorsi, che seguono dopo nella riga di comando.

## *Variabili*

Le variabili si impostano dopo le chiavi come una lista, formato di elementi è seguente:
*<variabile>=<valore>*

### *Alcune variabili più importanti:*

- `agent.language="C:\Program Files\DrWeb Enterprise Suite\RU-ESAUI.DWL"` — il parametro imposta la modalità di visualizzazione del menu contestuale di **Agent** in russo. Come valore si deve utilizzare il percorso completo al file di lingua (lingua predefinita è l'inglese).
- `spider.install=no` — non installare **SpIDer Guard.** Se non c'è variabile — installare.
- `spiderml.install=no` — analogo, non installare **SpIDer Mail**.
- `scanner.install=no` — analogo, non installare **Dr.Web**

**Scanner per Windows**.

- `spidergate.install=no` — analogo, non installare **SpIDer Gate**.
- `agent.id=`*<identificatore>*.
- `agent.password=`*<password>* — identificatore e password di workstation; se questi parametri sono impostati, la workstation si connette non come una workstation nuova, ma con i parametri indicati.

### *Server*

La lista dei **Server** è completamente analogo a quella descritta di **Agent**.

## H5. Dr.Web Enterprise Server

Ci sono alcuni varianti di comandi di avvio del **Server**, per comodità vengono descritte separatamente.

I comandi, riportati in H5.1 – H5.5, sono cross-piattaforma: si possono utilizzare sia nei SO Windows, sia nei SO della famiglia UNIX, se non indicato altrimenti.

### H5.1. Gestione di server Dr.Web Enterprise Server

`drwcsd [`*<chiavi>*`]` — configurare le impostazioni del funzionamento del **Server** (le chiavi vengono descritte in più dettagli sotto).

### H5.2. Comandi di base

- `drwcsd start` — avviare il **Server**.
- `drwcsd restart` — eseguire il riavvio completo del servizio del **Server** (eseguito come coppia `stop` e dopo `start`).

- `drwcsd stop` — normalmente terminare operazione del **Server**.
- `drwcsd reconfigure` — rileggere il file di configurazione e riavviarsi (si esegue più velocemente - senza avviare un nuovo processo).
- `drwcsd retemplate` — rileggere i template di avvisi dal disco.
- `drwcsd verifyakey` *<percorso_al_file>* – controllo correttezza di chiave di agent (`agent.key`).
- `drwcsd verifyekey` *<percorso_al_file>* – controllo correttezza di chiave del server (`enterprise.key`).
- `drwcsd verifyconfig` *<percorso_al_file>* – controllo sintassi del file di configurazione del **Server** (`drwcsd.conf`).
- `drwcsd stat` – mettere nel file di log le informazioni statistiche di funzionamento: tempo della CPU, utilizzo della memoria ecc. (per i SO della famiglia UNIX questo comando è analogo al comando `send_signal WINCH` oppure `kill SIGWINCH`).

## H5.3. Comandi di gestione del database

### *Inizializzazione del database*

`drwcsd [<chiavi>] initdb <chiave_di_Agent> [<script_del_database> [<file_ini> [<password>]]]` — inizializzazione del database.

- *<chiave_di_Agent>* — percorso alla chiave di licenza di **Enterprise Agent** `agent.key` (è obbligatorio indicare).
- *<script_del_database>* — script di inizializzazione del database. Valore speciale - (meno) significa non utilizzare lo script.
- *<file_ini>* — file, creato preliminariamente nel formato `drweb32.ini`, che imposterà una configurazione iniziale dei componenti del software di **Dr.Web** (per gruppo **Everyone**). Valore speciale - (meno) significa non utilizzare tale file.

- *<password>* — password iniziale di amministratore del **Server** (suo nome è **admin**). Di default è **root**.



Segno "meno" può essere omesso, se non ce ne sono parametri che lo seguono.

## *Impostazione dei parametri di inizializzazione del database*

Se si utilizza il database incorporato, i parametri di inizializzazione si possono impostare via il file esterno. Per farlo si utilizza il comando:

`drwcsd.exe initdbex` *<response-file>*

*<response-file>* - file, in cui sono scritti i parametri di inizializzazione del database, riga per riga, nello stesso ordine come parametri initdb.

Formato del file:

*<percorso_al_file_della_chiave>*
*<percorso_al_file_initdb.sql>*
*<percorso_al_file_drweb32.ini>*
*<password_amministratore>*



Si si utilizza nei SO Windows il response-file, si può utilizzare qualsiasi carattere nella password dell'amministratore.

Le righe di coda, che seguono il parametro necessario in questo caso, non sono obbligatorie. Se una riga rappresenta un "-" (un segno "meno"), si utilizza il valore predefinito (come in `initdb`).

## Aggiornamento del database

`drwcsd [<chiavi>] updatedb <script>` — eseguire qualsiasi manipolazione con un database (per esempio, aggiornamento durante cambio versione), eseguendo operatori SQL dal file *<script>*.

## Aggiornamento della versione del database

`drwcsd upgradedb <catalogo>` — avviare il **Server** per aggiornare la struttura del database se si passa alla nuova versione (v. catalogo `update-db`).

## Esportazione del database

`drwcsd exportdb <file>` — esportazione del database nel file indicato.

**Esempio per Windows:**

```
C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program Files
\DrWeb Enterprise Server\var" -verbosity=all
exportdb "C:\Program Files\DrWeb Enterprise Server
\esbase.es"
```

Nel SO **UNIX** azione viene eseguita a nome di utente `drwcs:drwcs` nel catalogo `$DRWCS_VAR` (oltre il SO **FreeBSD**, che salva di default il file nella directory, da cui è avviato lo script; se si indica esplicitamente il percorso, la directory deve essere provvista di diritti di scrittura per *<utente>*:*<gruppi>*, che sono stati creati all'installazione, di default - `drwcs:drwcs`).

### *Importazione del database*

`drwcsd importdb` *<file>* — importazione del database dal file indicato (contenuti precedenti vengono eliminati dal database).

### *Verifica del database*

`drwcsd verifydb` — avviare **Server** per la verifica del database. Alla fine della verifica il **Server** visualizza le informazioni sui risultati nel file di log (di default `drwcsd.log`).

## H5.4. Comandi per gestire il repositorio

- `drwcsd syncrepository` — eseguire la sincronizzazione del repositorio con **SAM**. Arrestare il **Server** prima di eseguire il comando!
- `drwcsd rerepository` — rileggere il repositorio dal disco.

## H5.5. Backup dei dati critici del Server Dr.Web Enterprise Server

Il backup dei dati critici del **Server** (contenuti del database, chiave di licenza del **Server**, chiave di codifica chiusa, file di configurazione del **Server** e del **Centro gestione**) viene creato con il seguente comando:

`drwcsd -home=`*<percorso>* `backup [`*<cartella>* `[`*<numero>*`]]` — dati critici del **Server** si copiano nella cartella indicata. `-home` imposta la cartella di installazione del **Server**. *<numero>* - numero di copie dello stesso file conservate.

**Esempio per il SO Windows:**

```
C:\Program Files\DrWeb Enterprise Server
\bin>drwcsd -home="C:\Program Files\DrWeb
Enterprise Server" backup C:\a
```

Le copie di riserva si salvano nel formato `.dz`, compatibile con `gzip` e altri archiviatori. Dopo la decompressione tutti i file, oltre i contenuti del database, si possono utilizzare. I contenuti del database, salvati nel backup, si possono importare in un altro database del **Server** con la chiave `importdb` e in questo modo ripristinare i dati (v. Ripristino del database di Dr.Web Enterprise Security Suite).

**ESS**, partendo dalla versione **4.32**, regolarmente salva le copie di backup di informazioni importanti in `\var\Backup` della cartella operativa del **Server**. Per farlo, in orario del **Server** è stato incluso un processo giornaliero, che esegue tale funzione. Se tale processo è assente dall'orario, si consiglia di crearlo. In particolare, il processo di backup dei dati critici non c'è, se inizialmente la versione del **Server** installata - **4.32**, e ulteriori versioni sono state installate su di essa.

## H5.6. Comandi, disponibili solo nel SO Windows®

- `drwcsd [<chiavi>] install` — installare il servizio del **Server** in sistema.
- `drwcsd uninstall` — eliminare il servizio del **Server** dal sistema.
- `drwcsd kill` — terminare il servizio del **Server** di emergenza (se non si è riusciti a farlo normalmente). Non si consiglia di utilizzare questo comando senza necessità assoluta.
- `drwcsd silent` — proibire visualizzazione dei messaggi dal **Server**. Si utilizza nei file di comando, per disattivare interattività di operazione del **Server**.

## H5.7. Comandi, disponibili solo nei SO della famiglia UNIX®

- `drwcsd config` – simile al comando `reconfigure` o `kill SIGHUP` – riavvio del **Server**.
- `drwcsd dumpimportdb` – registrare nel file del log del **Server** informazioni dettagliate di importazione nel database interno o esterno.
- `drwcsd interactive` – riavviare il **Server**, ma non passa la gestione al processo.
- `drwcsd newkey` – generare nuove chiavi di codifica (`drwcsd.pri` e `drwcsd.pub`).
- `drwcsd readtempl` – rileggere i moduli di avvisi dal disco.
- `drwcsd readrepo` – rileggere il repositorio dal disco.
- `drwcsd selfcert` – generare nuovo certificato SSL e chiave di codifica chiusa RSA (`certificate.pem`, `private-key.pem`).
- `drwcsd shell` *<nome_file>* – avvio del file binario.
- `drwcsd showpath` – visualizzare tutti i percorsi del programma, definiti nel sistema.
- `drwcsd status` – visualizzare lo stato attuale del **Server** (avviato, arrestato).

## H5.8. Descrizione delle chiavi

### *Chiavi cross-piattaforma*

- `-activation-key=`*<chiave_licenza>* — la chiave di licenza del **Server**. Di default è il file `enterprise.key` che si trova nella sottocartella `etc` della cartella radice.
- `-bin-root=`*<cartella_di_eseguibili>* — il percorso ai file eseguibili. Di default è la sottocartella `bin` della cartella radice.
- `-conf=`*<file_config>* — nome e posizione del file di configurazione del **Server**. Di default è il file `drwcsd.conf`

nella sottocartella `etc` della cartella radice.

- `-daemon` — per le piattaforme Windows significa l'avvio come servizio; per le piattaforme UNIX significa: "processo demone" (passare alla cartella radice, disconnettersi dal terminale e usare la modalità di background).
- `-db-verify=on` — all'avvio del **Server** controllare l'integrità del database. È il valore predefinito. Non è consigliato di avviare il programma se è indicato esplicitamente il valore opposto, ad eccezione dell'avvio subito dopo che il database è stato controllato tramite il comando `drwcsd verifydb`, vedi sopra.
- `-help` — visualizzare la guida. È simile ai programmi descritti sopra.
- `-hooks` — consentire al **Server** di eseguire script di estensione di utente che si trovano nella cartella:
  - in caso di SO Windows: `var\extensions`
  - in caso di SO FreeBSD e SO Solaris: `/var/drwcs/extensions`
  - in caso di SO Linux: `/var/opt/drwcs/extensions`

  della cartella di installazione di **Enterprise Server**. Gli script possono automatizzare il lavoro dell'amministratore, semplificare e accelerare l'esecuzione di alcuni compiti. Di default tutti gli script sono disabilitati.
- `-home=<radice>` — la cartella di installazione del **Server** (la cartella radice). La struttura di questa cartella è descritta nel punto Installazione di Dr.Web Enterprise Server per i SO Windows®. Di default è la cartella corrente all'avvio.
- `-log=<log>` — il nome del file di log del **Server**. Invece di un nome di file si può usare il segno "meno" (solo per **Server** sulle piattaforme UNIX) che significa "mostrare il log sul solito output". Di default: in caso delle piattaforme Windows è `drwcsd.log` nella cartella specificata dalla chiave `-var-root`, e in caso delle piattaforme UNIX si imposta dalla chiave `-syslog=user` (vedi sotto).
- `-private-key=<chiave_chiusa>` — la chiave chiusa del **Server**. Di default è `drwcsd.pri` nella sottocartella `etc`

della cartella radice.

- `-rotate=<N><f>,<M><u>` - modalità di rotazione del log del funzionamento di **Server**, dove:
  - <*N*> - il numero totale di file di log (compresi il file attuale e quelli di archivio);
  - <*f*> - il formato di memorizzazione dei file di log, i valori ammissibili sono `z` (gzip) - comprimere file, si usa di default, oppure `p` (plain) - non comprimere file;
  - <*M*> - dimensione del file;
  - <*u*> - unità di misura, i valori possibili sono `k` (kilo), `m` (mega), `g` (giga).

  Di default è `10,10m`, che significa: "custodire 10 file di 10 megabyte, comprimere file". Si può inoltre usare il formato speciale `none (-rotate=none)` che significa: "non usare la rotazione e registrare informazioni sempre nello stesso file di una dimensione illimitata".

  Se si usa la modalità di rotazione, si usa il seguente formato dei nomi di file: `file.<N>.log` oppure `file.<N>.log.dz`, dove <*N*> è il numero d'ordine: 1, 2 ecc.

  Per esempio, se il nome del file di log (v. la sopraindicata chiave `-log`) è stato impostato come `file.log`, allora:

  - `file.log` — è il file attuale (in cui si registrano le informazioni),
  - `file.1.log` — è il file precedente,
  - `file.2.log` e così via — il maggiore è il numero, la più vecchia è la versione del file di log.
- `-trace` — registrare informazioni di log dettagliate nel posto, dove è accaduto l'errore.
- `-var-root=`*<cartella_di_modificabili>* — il percorso alla cartella in cui il **Server** ha diritto di registrare informazioni e in cui si conservano file modificabili (per esempio, log e file del repository). Di default è la sottocartella `var` della cartella radice.
- `-verbosity=`*<livello_dettagli>* — il livello di dettagli del log. Di default è `WARNING`. I valori ammissibili sono: `ALL`,

DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT. I valori ALL e DEBUG3 sono sinonimi (v. anche Allegato L. Formato dei file del log).



Questa chiave determina il grado di dettagli da registrare nel file di log che si imposta dalla chiave -log (vedi sopra) che segue questa chiave. Lo stesso comando può includere più chiavi di questo tipo.

Le chiavi -verbosity e -log dipendono da posizione.

Se queste chiavi si usano contemporaneamente, la chiave -verbosity deve stare prima della chiave -log, perché la chiave -verbosity ridefinisce il livello di dettagli dei log che si trovano ai percorsi impostati più avanti nella riga di comando.

### *Chiavi ammissibili solo nei SO Windows*

- -minimized — (solo se si avvia non come servizio, ma in modo interattivo) — ridurre la finestra.
- -screen-size=<*dimensione*> — (solo se si avvia non come servizio, ma in modo interattivo) — la dimensione misurata in righe del log visibile nella finestra di **Server**, di default è 1000.

### *Chiavi ammissibili solo nei SO della famiglia UNIX*

- -etc=<*path*> – il percorso alla directory etc (<var>/etc).
- -pid=<*file*> — il file in cui il **Server** registra l'identificatore del suo processo.
- -syslog=<*modalità*> — registrazione del log nel registro di sistema. Le modalità possibili sono: auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp, local0 – local7 e in caso di alcune piattaforme — ftp, authpriv e console.



Le chiavi `-syslog` e `-log` funzionano insieme. Vuol dire che all'avvio del **Server** con la chiave `-syslog` (per esempio, `service drwcsd start -syslog=user`), il **Server** si avvierà con il valore impostato per la chiave `-syslog` e con il valore predefinito della chiave `-log`.

- `-user=`<*utente*>, `-group=`<*gruppo*> — sono disponibili solo per il SO UNIX, se il programma si avvia a nome dell'utente **root;** significano "cambiare l'utente o il gruppo del processo e eseguire il programma con i permessi dell'utente (gruppo) indicato".

## H5.9. Variabili, disponibili nei SO della famiglia UNIX®

Per semplificare la gestione del **Server** nei SO della famiglia UNIX a disposizione dell'amministratore sono le variabili, locate nel file di script `/etc/init.d/drwcsd`.

La corrispondenza tra variabili e chiavi di riga di comando per `drwcsd` è riportata in Tabella H-1.

**Tabella H-1.**

| Chiavi | Variabile | Parametri predefiniti |
|---|---|---|
| -home | DRWCS_HOME | • `/usr/local/drwcs` - per il SO FreeBSD,<br>• `/usr/drwcs` - per tutti gli altri SO. |
| -var-root | DRWCS_VAR | |
| -etc | DRWCS_ETC | $DRWCS_VAR/etc |
| -rotate | DRWCS_ROT | 10,10m |
| -verbosity | DRWCS_LEV | trace3 |
| -log | DRWCS_LOG | $DRWCS_VAR/log/drwcsd.log |

| Chiavi | Variabile | Parametri predefiniti |
|---|---|---|
| -conf | DRWCS_CFG | $DRWCS_ETC/drwcsd.conf |
| -pid | DRWCS_PID | |
| -user | DRWCS_USER | |
| -group | DRWCS_GROUP | |
| -hooks | DRWCS_HOOKS | |
| -trace | DRWCS_TRACE | |



Le variabili `DRWCS_HOOKS` e `DRWCS_TRACE` non hanno parametri. Durante impostazione di variabili le chiavi corrispondenti vengono aggiunte durante esecuzione dello script. Se variabili non sono impostate, chiavi non saranno aggiunte.

Altre variabili sono riportate in Tabella H-2.

**Tabella H-2.**

| Variabile | Parametri predefiniti | Descrizione |
|---|---|---|
| DRWCS_ADDOPT | | |
| DRWCS_CORE | unlimited | Dimensione massima del file nucleo. |
| DRWCS_FILES | 8192 | Numero massimo di descrittori di file, che può aprire **Server**. |
| DRWCS_BIN | $DRWCS_HOME/bin | Directory, da cui viene avviato `drwcsd`. |
| DRWCS_LIB | $DRWCS_HOME/lib | Directory con le librerie del **Server**. |

I valori di parametri predefiniti entrano in vigore, se tali variabili non sono definite nello script `/etc/init.d/drwcsd`.



Le variabili `DRWCS_HOME`, `DRWCS_VAR`, `DRWCS_ETC`, `DRWCS_USER`, `DRWCS_GROUP`, `DRWCS_HOOKS` sono già definite nel file di script `/etc/init.d/drwcsd`.

Se esiste già un file `${TGT_ES_ETC}/common.conf`, questo file viene incluso in `/etc/init.d/drwcsd`, il chè può redefinire alcune variabili, comunque, se esse non si esportano (con il comando `export`), non influiscono in nessun modo.

***Per impostare le variabili si deve:***

1. Aggiungere definizione di variabile nel file di script `/etc/init.d/drwcsd`.
2. Esportare la variabile con il comando `export` (impostato sempre lì).
3. Durante l'avvio di un altro processo ancora da questo script questo processo legge i valori predefiniti.

**Per esempio**:

Per modificare il livello di dettagli del log del **Server** al livello massimo:

1. Nel `/etc/init.d/drwcsd` aggiungere le seguenti righe:

```
DRWCS_LEV=ALL
export DRWCS_LEV
```

2. Avviare il **Server**, se era arrestato:

   `/etc/init.d/drwcsd start` (o `service drwcsd start`)

   O riavviare il **Server**, se è già stato avviato:

   `/etc/init.d/drwcsd restart` (o `service drwcsd restart`)

3. Il livello di dettagli del log avrà il valore `ALL`.

## H5.10. Configurazione di Dr.Web Enterprise Server per i SO della famiglia UNIX®

Durante l'installazione del **Server** nei SO della famiglia UNIX si deve eseguire la configurazione di alcuni parametri di configurazione del **Server**. La procedura di configurazione dei parametri di **Server** può essere iniziata manualmente (per farlo è necessario che sia installato l'ambiente perl). Per farlo, è sufficiente avviare lo script `configure.pl`, che si trova:

- nella directory `/usr/local/drwcs/bin/` per i SO **FreeBSD**,
- nella directory `/opt/drwcs/bin/` per i SO **Linux** e **Solaris**.

***Formato di comando di avvio:***

`configure.pl` *<chiavi>*

***Chiavi disponibili:***

- `--proxy server=`*<proxy_server>* – impostare indirizzo del server proxy.
  - user=*<proxy_user>* – indicare nome utente del server proxy.
  - password=*<proxy_password>* – indicare la password per utente del server proxy.
- `--stat server=`*<stat_server>* – impostare indirizzo del server di statistiche (predefinito `stat.drweb.com:80`).
  - url=*<url_on_server>* – impostare URL sul server di statistiche (predefinito `/update`).
  - interval=*<send_interval>* – impostare intervallo di invio statistiche.
- `--initbase` – inizializzare il database del **Server**.
- `--upgradebase` – aggiornare database sul **Server**.
- `--interactive` – avviare in modalità interattiva.
- `--skip proxy=1` – saltare uno dei passi in modalità interattiva.

- `stat=1 |`
- `initbase=1 |`
- `upgradebase=1`

- `--verbose` – visualizzare le informazioni dettagliate.
- `--help | ?` – visualizzare la guida su configurazioni del comando.

## H6. Utilità di amministrazione del database incorporato

Utilità di amministrazione del database incorporato si trova nelle seguenti directory:

- per i SO **Linux** e **Solaris**: `/opt/drwcs/bin`
- per il SO **FreeBSD**: `/usr/local/drwcs/bin`
- per il SO della famiglia **Windows**:

  *<cartella_di_installazione_del_Server>*`\bin`

  (di default la cartella di installazione del **Server**: `C:\Program Files\DrWeb Enterprise Server`).

***Formato di comando di avvio:***

`drwidbsh` *<percorso_al_file_del_database>*

Il programma opera nella modalità testo di dialogo, aspetta input da utente dei comandi di programma (comandi iniziano con il punto).

Per la guida ad altri programmi inserire `.help`. Viene visualizzato il testo di guida.

Per le informazioni dettagliate utilizzare i manuali di guida sulla lingua SQL.

# H7. Utilità di generazione di copie di chiavi e di firma digitale

***Nomi e location dei file delle chiavi di codifica nella cartella di installazione del Server:***

- `\etc\drwcsd.pri` - chiusa,
- `\Installer\drwcsd.pub` - aperta.

***Varianti del formato di comando:***

- `\bin\drwsign check [-public-key=<aperta>] <file>` – verificare la firma del file, utilizzando *<aperta>* come chiave aperta di persona che ha firmato tale file.
- `\bin\drwsign extract [-private-key=<chiusa>] <aperta>` – estrae la chiave aperta dal file della chiave chiusa del formato complesso (versione **4.33** e ulteriori).
- `\bin\drwsign genkey [<chiusa> [<aperta>]]` – genera una copia chiave aperta-chiave chiusa e le scrive nei file corrispondenti.



La versione di utilità per le piattaforme Windows (a differenza della versione per i SO UNIX) non protegge in nessun modo la chiave chiusa da creazione delle copie.

- `\bin\drwsign help [<comando>]` – guida breve al programma e al formato di riga di comando.
- `\bin\drwsign join432 [-public-key=<aperta>] [-private-key=<chiusa>] <nuova_chiusa>` – unisce le chiavi aperta e chiusa del formato di versione **4.32** in un nuovo formato complesso di chiave chiusa di versione **4.33** e superiori.
- `\bin\drwsign sign [-private-key=<chiusa>] <file>` – firmare file *<file>*, utilizzando la chiave chiusa indicata.

## H8. Gestione Server Dr.Web Enterprise Server nei SO della famiglia UNIX® con il comando kill

**Server** nei SO UNIX viene gestito dai segnali, inviati al processo del **Server** da utilità `kill`.



La guida dettagliata su utilità `kill` è disponibile con il comando `man kill`.

***Sotto si riporta la lista dei segnali di utilità e delle azioni da essi eseguite:***

- `SIGWINCH` - output nel file del log di statistiche di operazione (tempo CPU, utilizzo di memoria ecc.),
- `SIGUSR1` - rilettura del repositorio dal disco,
- `SIGUSR2` - rilettura dei moduli di avvisi dal disco,
- `SIGHUP` - riavvio del **Server**,
- `SIGTERM` - arresto del **Server**,
- `SIGQUIT` - arresto del **Server**,
- `SIGINT` - arresto del **Server**.

Azioni analoghe per **Server** nei SO Windows vengono realizzati con le chiavi di comando `drwcsd`, v. Allegato H5.3.

## H9. Scanner Dr.Web per il SO Windows®

Questo componente del software di workstation ha i parametri di riga di comando, descritti nel manuale dell'utente **Dr.Web® Anti-virus per Windows**. Unica differenza è che durante l'avvio di **Scanner Agent** passa a **Scanner** i parametri `/go /st` automaticamente e in ordine obbligatorio.

# H10. Server proxy

Per configurare alcuni parametri del **Server proxy** avviare con le chiavi corrispondenti il file eseguibile `drwcsd-proxy`, che si trova:

- nei SO Windows: nella cartella di installazione del **Server proxy**.
- Per i SO della famiglia UNIX: nella sottocartella `bin` della cartella di installazione del **Server proxy**.

### *Formato di comando di avvio:*

`drwcsd-proxy` <*chiavi*>

### *Chiavi disponibili:*

- `--help` – visualizzare la guida per le chiavi per configurare **Server proxy**.
- `--daemon` – solo per i SO della famiglia UNIX: avviare **Server proxy** nella modalità di demone.
- `--control` <*arg*> – solo per i SO Windows: impostare i parametri di configurazione del servizio.

  Parametri disponibili:

  - `run` – (predefinito) avviare il **Server proxy** nella modalità background come il servizio del SO Windows.
  - `install` – installare **Server proxy**.
  - `uninstall` – eliminare **Server proxy**.
- `--cfg` <*path*> – impostare il percorso al file di configurazione del **Server proxy**.
- `--pool-size` <*N*> – dimensione del pool per connessioni di client. Di default 2.
- `--trace` – attivare logging dettagliato di richiami al **Server proxy**. Disponibile solo se assemblaggio del **Server proxy** supporta il logging dettagliato di stack di chiamate.
- `--use-console-log` – gestire il log di operazione del **Server proxy** in console.

- `--use-file-log` *<file>* – scrivere il log di operazione del **Server proxy** in file, dove *<file>* - percorso al file di log.
- `--rotate=`*<N><f>*, *<M><u>* – modalità di rotazione del log di operazione del **Server proxy**, dove:
  - *<N>* – numero totale dei file di log (compresi attuale e quelli di archivio);
  - *<f>* – formato di registrazione del file di log, valori disponibili: `z` (gzip) – comprimere file, utilizzato di default, o `p` (plain) – non comprimere file;
  - *<M>* – dimensione di file;
  - *<u>* – unità di misura, valori disponibili: `k` (kilo), `m` (mega), `g` (giga).

  Di default `10,10m`, il chè significa conservare 10 file per 10 megabyte, utilizzare compressione.
- `--verbosity=`*<livello_dettagli>* – livello di dettagli del log. Di default `TRACE3`. Valori disponibili: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. Valori `ALL` e `DEBUG3` – sinonimi.



Tutte le chiavi per impostare i parametri di operazione del **Server proxy** si possono indicare contemporaneamente.

Output del log di operazione contemporaneamente in file e in console non è supportato. In questo caso:

- Se nessuna chiave è impostata, il log viene gestito in console.
- Se sono impostate tutte e due le chiavi, il log viene scritto in file.

# Allegato I. Variabili di ambiente, esportate da Server Dr.Web Enterprise Server

Per semplificare configurazione dei processi, avviati da **Enterprise Server** su orario, si richiedono le informazioni su location delle cartelle del **Server**. A questa fine il **Server** esporta in ambiente dei processi avviati le seguenti variabili:

- `DRWCSD_HOME` — percorso alla cartella radice (cartella di installazione). Nome di chiave `-home`, se è stato impostato durante l'avvio del **Server**, altrimenti la cartella corrente durante l'avvio.
- `DRWCSD_EXE` — percorso alla cartella dei file eseguibili. Valore di chiave `-bin-root`, se è stato impostato durante l'avvio del **Server**, altrimenti la sottocartella `bin` della cartella radice.
- `DRWCSD_VAR` — percorso alla cartella, dove **Server** ha il diritto di registrazione e che è destinato per conservare i file modificati (per esempio, log e file di repositorio). Valore di chiave `-var-root`, se è stato impostato durante l'avvio del **Server**, altrimenti la sottocartella `var` della cartella radice.

# Allegato J. Utilizzo di script di installazione iniziale per Dr.Web Enterprise Agent

Lo scenario del processo di installazione iniziale di **Agent** su workstation con installazione di rete (`drwinst.exe`) viene definito dal file `install.script`. Tali file si trovano nel catalogo radice dei prodotti nel repositorio. Nella fornitura standard essi sono presenti nelle cartelle `10-drwupgrade` e `20-drwagntd` e descrivono installazione predefinita.

Se nel catalogo c'è il file `.custom.install.script`, viene utilizzato proprio questo file invece dello scenario standard.



I file con qualsiasi altro nome, che inizia con punto, non vengono aggiornati durante aggiornamento del prodotto e non influiscono su operazione del repositorio.

***Conseguenza di azioni durante l'installazione iniziale:***

1. Installazione di rete richiede dal **Server** installazione di piattaforme: `win-setup`, `common`, `win`, `win-nt` e `win-9x` — questa è la lista di piattaforme standard in ordine predefinito. L'ordine di conseguenza di piattaforme può essere modificato con la chiave `-platforms=p1,p2,p3...` richiamando `drwinst`. La piattaforma `win-setup` non rientra nella fornitura standard ed è destinata per creare, se è necessario, propri scenari di installazione.
2. **Server** crea a secondo della lista di piattaforme la lista dei file, di conseguenza vedendo tutti i prodotti in ordine alfabetico e le liste dei file, creati dalle costruzioni `files{ }` per questa piattaforma nello scenario di installazione `install.script` (v. sotto). In parallelo viene costruito lo script complessivo sulla base delle costruzioni `scripts{ }`.
3. **Server** ottiene la lista generale dei file e lo script complessivo.

4. **Server** invia i file e lo script, che viene eseguito da installazione di rete.

Adesso vediamo lo stesso `install.script` con esempio di catalogo `20-drwagntd`.

```
; master part of installation: Agent & its stuff.
; drwscr.dll goes with upgrader, so unlisted here.

platform{  ; win - for all Windows OS
           ; `name: XXX' MUST go first!

   name: win  ; (mandatory stanza)
              ; this platform name

              ; include, scripts{ }, files{ }
              ; can go in any order

   scripts {  ; (optional)
              ; script being merged with all others
win.inst.rexx ; and executed after transfer all
              ; files for all platforms requested
              ; by installer
              ; Windows installer request order:
              ; - win-setup (optional! for
              ;              customization)
              ;   - common
              ;   - win
              ;   - win-nt OR win-9x
         }

   files {    ; (optional)
              ; this platform files being
              ; transfered to installer
          win/uninstall.rexx
          win/drwinst.exe
```

```
          win/drwagntd.exe
          win/drwagnui.exe
          win/drwhard.dll
        }
}

platform {    ; win-9x - for Windows 95-ME
   name: win-9x
   scripts{ win-9x.inst.rexx }
}

platform {    ; win-nt - for Windows NT-2003
   name: win-nt
   scripts{ win-nt.inst.rexx }
}

platform{        ; common - for any OS including
UNICES
    name: common
    scripts { common.inst.rexx }
}

; include file.name ; (optional)
     ; this stanza tells to include other file.
     ; including file will be searched in the
     ; same directory where current file are
     ; located if `file.name' does not include
     ; directory specificator
```

Lo script rappresenta la lista di costruzioni `platform{ }` e permette con la costruzione `include` includere definizioni da altri file (`include` è ammissibile solo al livello superiore e non è ammissibile all'interno di `platform{ }`). Se `file.name` nel `include` non contiene i percorsi, ma solo nome del file, viene cercato nello stesso catalogo di quello attuale.

Possono essere presenti le proprie costruzioni `include` in file inclusi.

La descrizione di piattaforma si inizia con la costruzione `name: XXX`. Dopo segue un paio di liste `files{ }` e `scripts{ }`. L'ordine di visualizzazione di queste liste non è importante; le liste possono contenere qualsiasi numero di elementi. L'ordine di elementi nella lista è importante, perché definisce l'ordine di passaggio dei file a workstation e la costruzione dello script creato.

L'ordine di visualizzazione di costruzioni `platform{ }` non è neanche importante.

Di seguito sono elencate le variabili di script di installazione (i valori a queste variabili possono essere assegnati dalla riga di comando di installazione di rete) e i loro valori predefiniti:

- `spider.install = 'yes'`
- `spiderml.install = 'yes'`
- `scanner.install = 'yes'`
- `install.home` — cartella di installazione
- `agent.logfile = install.home'\logs \drwagntd.log'`
- `agent.loglevel = 'trace'`
- `agent.logrotate = '10,10m'`
- `agent.servers = install.servers`
- `agent.serverkey = install.home'\drwcsd.pub'`
- `agent.compression = 'possible'`
- `agent.encryption = 'yes'`
- `agent.findretry = '3'`
- `agent.findtimeout = '5'`
- `agent.spiderstatistics = '30'`
- `agent.importantmsg = '2'`
- `agent.discovery = 'udp/:2193'`
- `agent.startmsg = '2'` (o `agent.startmsg = 'NONE'`)

Il parametro `agent.importantmsg` definisce, se all'utente viene visualizzato un errore di aggiornamento, necessità di riavvio ecc. **0** — non visualizzare avviso, **1** — visualizzare un avviso di informazione popup.

***Andiamo a creare uno scenario di installazione non standard, dove non si installa SplDer Guard e si imposta il logging con il massimo livello di dettagli:***

1. Creare `20-drwagntd` file `.win-setup.inst.rexx` e scrivere in esso:

```
spider.install = 'no'
agent.loglevel = 'all'
```

2. Creare in `20-drwagntd` file `.custom.install.script` e scrivere in esso

```
include install.script

platform{
      name: win-setup
      scripts{ .win-setup.inst.rexx }
}
```

3. Riavviare il **Server** o dare il segnale di riavviare il repositorio:
   - per il SO **UNIX**: `kill -USR1 cat `drwcsd.pid``
   - per il SO **Windows**: `drwcsd.exe rerepository`

# Allegato K. Utilizzo di espressioni regolari in Dr.Web Enterprise Security Suite

Alcuni parametri di **Dr.Web ESS** si impostano nel formato di espressioni regolari. Elaborazione di espressioni regolari viene eseguita con la libreria di programma PCRE.

La descrizione dettagliata di sintassi della libreria PCRE è disponibile sul server http://www.pcre.org/.

In questo allegato è riportata solo una breve descrizione dei punti principali di utilizzo delle espressioni regolari.

## K1. Opzioni di espressioni regolari

Le espressioni regolari vengono utilizzate sia nel file di configurazione di **Server**, sia in **Centro gestione** quando nelle impostazioni di **Scanner** si definiscono oggetti da escludere dalla scansione.

Le espressioni regolari si scrivono nella seguente forma:
`qr{EXP}options`

dove `EXP` è l'espressione stessa, `options` è una sequenza di opzioni (stringa di lettere), `qr{}` è metacaratteri letterali. In generale la costruzione si vede, per esempio, così:
`qr{pagefile\.sys}i` – file di swap di SO Windows NT

Sotto sono descritte opzioni e le espressioni regolari stesse. Per una descrizione più dettagliata vedere http://www.pcre.org/pcre.txt.

- Opzione `'a'`, che corrisponde a `PCRE_ANCHORED`

  Con quest'impostazione il pattern "getta l'ancora" forzatamente, cioè si limita a confrontare solo la prima posizione da cercare nella stringa in base a cui si esegue la ricerca ("stringa di

oggetto"). Ciò può anche essere raggiunto tramite costruzioni appropriate del pattern stesso.

- Opzione `'i'`, che corrisponde a `PCRE_CASELESS`

  Con quest'impostazione le lettere del pattern vengono confrontate sia con lettere maiuscole, sia con quelle minuscole. Questa possibilità può essere modificata nel pattern impostando l'opzione `(?i)`.

- Opzione `'x'`, che corrisponde a `PCRE_EXTENDED`

  Con quest'impostazione vengono ignorati gli spazi fra caratteri nel pattern, ad eccezione dei casi, in cui essi sono preceduti da caratteri di controllo oppure si trovano dentro una classe di caratteri. Lo spazio non include il carattere `VT` (codice 11). Inoltre vengono ignorati i caratteri che si trovano fuori di una classe di caratteri tra il carattere `#`, non preceduto da un carattere di controllo, e il carattere di nuova stringa, quello compreso. Quest'opzione può essere modificata nel pattern impostando l'opzione `(?x)`. Quest'impostazione rende possibile inserire commenti dentro pattern compositi. Si tiene presente che questo è applicabile solo ai caratteri d'informazione. I caratteri di spazio non possono stare nel pattern dentro sequenze di caratteri speciali, per esempio, dentro la sequenza `(?(` la quale introduce subpattern condizionale.

- Opzione `'m'`, che corrisponde a `PCRE_MULTILINE`

  Di default, PCRE considera che la stringa di oggetto consista di una sola stringa di caratteri (anche se in realtà essa contiene caratteri di nuove stringe). Il metacarattere di *"inizio stringa"* `"^"` viene confrontato solo all'inizio della stringa, mentre il metacarattere *"fine stringa"* `"$"` viene confrontato solo alla fine della stringa oppure prima della nuova stringa finale (se non è impostata l'opzione `PCRE_DOLLAR_ENDONLY`).

  Se è impostata l'opzione `PCRE_MULTILINE`, i metacaratteri *"inizio stringa"* e *"fine stringa"* si attaccano a qualsiasi nuova stringa che viene direttamente prima o dopo di essi nella stringa di oggetto, e anche all'inizio e alla fine della stringa. Quest'opzione può essere modificata nel pattern impostando

l'opzione `(?m)`. Se il testo non contiene caratteri `"\n"` oppure se il pattern non contiene `^` o `$`, l'opzione `PCRE_MULTILINE` non ha senso.

- Opzione `'u'`, che corrisponde a `PCRE_UNGREEDY`

  Quest'opzione annulla "l'avidità" dei quantificatori in modo che essi diventano "non avidi" di default, ma ripristinano "l'avidità" se sono seguiti da `"?"`. Questa possibilità può anche essere configurata tramite l'opzione `(?U)` nel pattern.

- Opzione `'d'`, che corrisponde a `PCRE_DOTALL`

  Con quest'impostazione il metacarattere di punto nel pattern viene confrontato con tutti i caratteri, compreso il carattere di nuova stringa. Senza di esso i caratteri di nuova stringa vengono esclusi. Quest'opzione può essere modificata nel pattern impostando la nuova opzione `(?s)`. Una classe negativa, per esempio `[^a]` viene sempre confrontata con il carattere di nuova stringa, a prescindere dalle impostazioni di quest'opzione.

- Opzione `'e'`, che corrisponde a `PCRE_DOLLAR_ENDONLY`

  Con quest'impostazione il carattere di dollaro nel pattern viene confrontato solo alla fine della stringa di oggetto. Senza quest'opzione il carattere di dollaro viene confrontato anche nella posizione direttamente prima del carattere di nuova stringa alla fine della stringa (ma non davanti a qualsiasi altro carattere della nuova stringa). L'opzione `PCRE_DOLLAR_ENDONLY` viene ignorata se è impostata l'opzione `PCRE_MULTILINE`.

## K2. Particolarità delle espressioni regolari PCRE

*Espressione regolare* - è un modello, confrontato con il testo da sinistra a destra. Maggior parte dei caratteri nel modello significano se stessi e vengono applicati ai caratteri corrispondenti nel testo.

Vantaggio principale di espressioni regolari sta nella possibilità di includere nel modello varianti e ripetizioni. Vengono codificati con i metacaratteri che non significano se stessi ma, invece, vengono

interpretati nel modo particolare.

Esistono due set di metacaratteri diversi: quelli che si utilizzano fra parentesi quadre e quelli che si utilizzano fuori parentesi quadre. Li vediamo separatamente in dettagli. Fuori parentesi quadre si utilizzano i seguenti metacaratteri:

- `\` carattere standard di gestione (`escape`), che permette alcune varianti di applicazione,
- `^` dichiara inizio linea (o testo nella modalità multilinea),
- `$` dichiara fine linea (o testo nella modalità multilinea),
- `.` corrisponde a qualsiasi carattere, oltre il carattere da capo (predefinito),
- `[` inizio descrizione classe dei caratteri,
- `]` fine descrizione classe dei caratteri,
- `|` inizio ramo alternativo,
- `(` inizio sottomodello,
- `)` fine sottomodello,
- `?` estende il valore `(`,

  inoltre quantificatore 0 o 1,

  inoltre quantificatore minimizzatore;
- `*` 0 o più,
- `+` 1 o più,

  anche "quantificatore possessivo",
- `{` inizio di quantificatore minimale/massimale.

La parte di modello tra parentesi quadre si chiama "classe di caratteri". In classe di caratteri i metacaratteri sono:

- `\` carattere standard di gestione (`escape`),

^ nega classe, ma solamente se all'inizio di classe,

– definisce range dei caratteri,

[ classe dei caratteri POSIX (solo se seguito da sintassi POSIX),

] chiude la classe dei caratteri.

# Allegato L. Formato dei file del log

I file del log del **Server** (v. Gestione log del server) e **Agent** vengono gestiti nel formato di testo, dove ogni riga rappresenta un avviso separato.

Il formato di riga di avviso è seguente:

*<anno><mese><giorno>*
*.<ora><minuto><secondo>.<centesimi_del_secondo>*
*<tipo_avviso>* [*<id_processo>*] *<nome_flusso>* [*<fonte_avviso>*]
*<avviso>*

dove:

- *<anno><mese><giorno>*
  *.<ora><minuto><secondo>.<centesimi_del_secondo>* – data precisa di scrittura di avviso nel file del log.
- *<tipo_avviso>* – livello del log:
  - **ftl** (fatal error – errore fatale) – avvisi di errori critici di funzionamento;
  - **err** (error – errore) – avvisi di errori di funzionamento;
  - **wrn** (warning – avviso) – avvisi di errori;
  - **ntc** (notice – commento) – avvisi informativi importanti;
  - **inf** (info – informazione) – avvisi informativi;
  - **tr0..3** (trace0..3 – tracing) – tracciamento di eventi con i vari livelli di dettagli (**Tracing3** – livello massimo dei dettagli);
  - **db0..3** (debug0..3 – debugging) – avvisi di debugging con i vari livelli di dettagli (**Debugging3** – livello massimo dei dettagli).

  Gli avvisi con il livello del log **tr0..3** (tracing) e **db0..3** (debugging) vengono fatti solamente per i sviluppatori del software di **Dr. Web ESS**.

- [*<id_processo>*] – identificatore numerico unicale del processo, nel quadro del quale è stato eseguito il flusso, che ha

scritto avviso nel file del log. In alcuni SO [<*id_processo*>] può essere presentato come [<*id_processo*> <*id_flusso*>].

- <*nome_flusso*> – indicazione caratteristica di flusso, nel quadro di quale è stata eseguita la scrittura di avviso nel file del log.
- [<*fonte_avviso*>] – indicazione del sistema, che ha iniziato a scrivere avviso nel file del log. La fonte non è sempre presente.
- <*avviso*> – descrizione di testo di azioni secondo il livello del log. Può comprendere sia la descrizione formale di avviso, sia i valori di alcune variabili importanti per tale caso concreto.

***Per esempio:***

**1)** `20081023.171700.74 inf [001316] mth:12 [Sch] Job "Purge unsent IS events" said OK`

dove:

- `20081023` – <*anno*><*mese*><*giorno*>,
- `171700` – <*ora*><*minuto*><*secondo*>,
- `74` – <*centesimi_del_secondo*>,
- `inf` – <*tipo_avviso*> - avviso informativo,
- `[001316]` – [<*id_processo*>],
- `mth:12` – <*nome_flusso*>,
- `[Sch]` – [<*fonte_avviso*>] - schedulatore,
- `Job "Purge unsent IS events" said OK` – <*avviso*> di corretta esecuzione del processo **Eliminazione di avvisi non inviati**.

**2)** `20081028.135755.61 inf [001556] srv:0 tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193`

dove:

- `20081028` – <*anno*><*mese*><*giorno*>,
- `135755` – <*ora*><*minuto*><*secondo*>,
- `61` – <*centesimi_del_secondo*>,
- `inf` – <*tipo_avviso*> - informativo,

- `[001556]` – [*<id_processo>*],
- `srv:0` – *<nome_flusso>*,
- `tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193` – *<avviso>* di stabilimento di una nuova connessione via il socket indicato.

# Allegato M. Descrizione di procedure dell'utente

Per semplificare e automatizzare esecuzione di certi processi di **Enterprise Server** si possono applicare le procedure dell'utente, realizzate come script lua. Questi script si devono trovare nella cartella:

- per il SO Windows: `var\extensions`
- per i SO FreeBSD e Solaris: `/var/drwcs/extensions`
- per il SO Linux: `/var/opt/drwcs/extensions`

della cartella di installazione del **Server**. Dopo l'installazione del **Server** in questa cartella si collocano tutte le procedure predefinite, che si possono utilizzare durante l'operazione. Per poter eseguirle il **Server** deve essere avviato con la chiave `-hooks`.

Tutti gli script di default sono disattivati. Per attivare gli script si deve nel file di script eliminare il parametro iniziale `disabled` o tutto il commento completamente (lasciare una riga vuota).

Cartella `extensions` contiene i seguenti script:

- `access_check.ds` – richiamato prima del controllo di accesso secondo ACL corrispondenti (Access Control List - liste di controllo degli accessi);
- `access_denied.ds` – richiamato durante il blocco di accesso secondo le configurazioni ACL o secondo il risultato di esecuzione del procedura `access_check`;
- `admin_logged.ds` – richiamato durante autorizzazione di amministratore completata con successo nel **Centro gestione**;
- `admin_noauth.ds` – richiamato durante errore di autorizzazione dell'amministratore nel **Centro gestione**;
- `agent_status.ds` – richiamato durante comunicazione da **Agent** delle sue politiche locali;
- `backup.ds` – richiamato dopo il completamento del backup, ma prima di eliminare i file del backup precedente;

- `bad_connection.ds` – richiamato se non è possibile stabilire una connessione al client;
- `connection_denied.ds` – richiamato durante il blocco di una nuova connessione secondo le limitazioni di accordo di licenza;
- `database_load.ds` – richiamato dopo il completamento del processo di caricamento del driver di database;
- `database_verify.ds` – richiamato dopo il completamento di verifica del database;
- `deinstallation.ds` – richiamato dopo il completamento di eliminazione di **Agent**;
- `disconnected.ds` – richiamato dopo il completamento di connessione al client;
- `group_changed.ds` – richiamato alla modifica di configurazioni del gruppo;
- `group_created.ds` – richiamato alla creazione di un gruppo nuovo;
- `group_deleted.ds` – richiamato all'eliminazione di un gruppo;
- `install.ds` – richiamato al ricevimento di evento `installation`;
- `installed_components.ds` – richiamato quando **Agent** comunica la lista dei componenti, installati su workstation;
- `jobexecuted.ds` – richiamato al ricevimento da **Agent** di evento `job executed`;
- `license_error.ds` – richiamato se non non è possibile stabilire una connessione al client secondo le limitazioni di accordo di licenza;
- `load_plugin.ds` – richiamato dopo il carico di plugin;
- `load_protocol.ds` – richiamato dopo il carico del plugin del protocollo;
- `neighbor_connected.ds` – richiamato alla connessione al **Server**;
- `neighbor_install.ds` – richiamato al ricevimento di evento `installation` da **Server** vicino;

- `neighbor_noauth.ds` – richiamato dopo il rifiuto di una connessione al **Server** per causa di errore di autorizzazione;
- `neighbor_run_begin.ds` – richiamato al ricevimento di evento `component started` da **Server** vicino;
- `neighbor_run_end.ds` – richiamato al ricevimento di evento `component completed` da **Server** vicino;
- `neighbor_scan_error.ds` – richiamato al ricevimento di evento `scan error` da **Server** vicino;
- `neighbor_scan_statistics.ds` – richiamato al ricevimento di evento `scan statistics` da **Server** vicino;
- `neighbor_station_status.ds` – richiamato al ricevimento da **Server** vicino delle politiche locali/configurazioni di workstation;
- `neighbor_virus.ds` – richiamato al ricevimento di evento `virus detected` dal **Server** vicino;
- `newbie_accepted.ds` – richiamato alla fornitura di accesso ad una workstation nuova, sua autorizzazione completata con successo e creazione di workstation nel database;
- `newbie_came.ds` – richiamato alla connessione di una nuova workstation;
- `newbie_registered.ds` – richiamato dopo aver fornito accesso ad una nuova workstation, ma prima di registrare le informazioni corrispondenti nel database;
- `pong.ds` – richiamato al ricevimento di `PONG` da client;
- `run_begin.ds` – richiamato al ricevimento di evento `component started` da **Agent**;
- `run_end.ds` – richiamato al ricevimento di evento `component completed` da **Agent**;
- `scan_error.ds` – richiamato al ricevimento di evento `scan error` da **Agent**;
- `scan_statistics.ds` – richiamato al ricevimento di evento `scan statistics` da **Agent**;
- `server_jobexecuted.ds` – richiamato dopo l'esecuzione del processo sul **Server**;
- `server_load.ds` – richiamato dopo il carico del file binario

del **Server** per eseguire alcune funzioni di servizio (**Server** non servirà i client);

- `server_start.ds` – richiamato durante l'avvio del **Server** e della sua disponibilità a servire i client;
- `server_terminate.ds` – richiamato dopo il completamento di servizio dei client da **Server**;
- `server_unload.ds` – richiamato dopo il completamento di esecuzione di alcune funzioni di servizio da **Server** (**Server** non ha servito client);
- `station_connected.ds` – richiamato alla connessione ad **Agent** completata con successo;
- `station_create.ds` – richiamato al completamento di creazione di workstation;
- `station_date.ds` – richiamato al rilevamento di scorrette ora/data di workstation;
- `station_deleted.ds` – richiamato durante eliminazione di workstation;
- `station_noauth.ds` – richiamato dopo il rifiuto di una connessione ad **Agent** per causa di errore di autorizzazione;
- `station_update_failed.ds` - richiamato dopo il ricevimento di avviso da **Agent** su errore di aggiornamento di workstation;
- `station_update_reboot.ds` - richiamato dopo il ricevimento di avviso da **Agent** su necessità di riavviare workstation dopo l'aggiornamento;
- `unload_plugin.ds` – richiamato durante estrazione del plugin;
- `unload_protocol.ds` – richiamato durante estrazione del plugin del protocollo;
- `virus.ds` – richiamato al ricevimento di evento `virus detected` da **Agent**;
- `virusbases.ds` – richiamato durante l'invio da **Agent** delle informazioni su database dei virus.

# Allegato N. Integrazione XML Web API e Dr.Web Enterprise Security Suite



La descrizione di **XML Web API** è riportata nel manuale **XML API per Dr.Web® Enterprise Security Suite** (v. anche Guida).

### *Applicazione*

Durante l'integrazione di **XML Web API** e **Dr.Web Enterprise Security Suite** si forniscono le funzioni per operare con utenze e automatizzare il processo di amministrazione di utenti del servizio. Si può utilizzarlo, per esempio, durante la creazione di pagine dinamiche per ottenere una richiesta dall'utente e passargli un file di installazione.

### *Autenticazione*

Per interazione con **Enterprise Server** si utilizza il log HTTP(S). XML API accetta le richieste RESET e ritorna XML. Per accedere a XML API si utilizza autenticazione HTTP di base (secondo lo standard RFC 2617). Se non si rispetta lo standard RFC 2617, HTTP(S) il server non richiederà i dati di utenza del client (nome di registrazione e password dell'amministratore di **Dr.Web ESS**).

# Allegato O. Procedure di autenticazione degli amministratori



Le informazioni fondamentali sull'autenticazione degli amministratori per connettersi a **Enterprise Server** sono riportate nella sezione Autenticazione di amministratori.

## Autenticazione se si usa Active Directory

Vengono configurati solo il permesso di uso e l'ordine nella lista di autenticatori: i tag `<enabled/>` e `<order/>` in `auth-ads.xml`.

***Come funziona:***

1. L'amministratore definisce lo username e la password in uno dei seguenti formati:
   - `username`,
   - `domain\username`,
   - `username@domain`,
   - LDAP DN dell'utente.
2. Con questo username e con questa password il server si registra sul controller di dominio predefinito (o sul controller di dominio che corrisponde al dominio specificato nello username).
3. Se la registrazione non è riuscita, si passa al meccanismo di autenticazione seguente.
4. Viene determinato LDAP DN dell'utente registrato.
5. Presso l'oggetto che ha il DN calcolato viene letto l'attributo `DrWeb_Admin`. Se è impostato come `FALSE`, significa l'insuccesso e si passa al meccanismo di autenticazione seguente.
6. Viene letto l'attributo `DrWeb_AdminReadOnly`. Se è impostato come `TRUE`, l'amministratore ha diritti di sola lettura.

7. Viene letto l'attributo `DrWeb_AdminGroupOnly`. Se è impostato come `TRUE`, l'amministratore ha diritti solo di gestire determinati gruppi.
8. Viene letto l'attributo `DrWeb_AdminGroup` che deve contenere una lista di gruppi da essere gestiti da questo amministratore.
9. Se in questa fase alcuni attributi non sono determinati, essi vengono cercati nei gruppi di cui fa parte questo utente. Per ciascun gruppo vengono controllati anche i suoi gruppi padre (strategia di ricerca in profondità).



In caso di qualsiasi errore si passa al meccanismo di autenticazione seguente.

L'utilità `drwschema-modify.exe` (fa parte della distribuzione di **Server**, si trova nella cartella `bin` della cartella di installazione di **Server**) crea una nuova classe di oggetti `DrWebEnterpriseUser` per Active Directory e descrive nuovi attributi per questa classe.

Gli attributi hanno OID nello spazio **Enterprise** come seguono:

```
#define DrWeb_enterprise_OID       "1.3.6.1.4.1"
#define DrWeb_DrWeb_OID            DrWeb_enterprise_OID
#define DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID
#define DrWeb_Alerts_OID           DrWeb_EnterpriseSuite_OI
#define DrWeb_Vars_OID             DrWeb_EnterpriseSuite_OI
#define DrWeb_AdminAttrs_OID       DrWeb_EnterpriseSuite_OI

// 1.3.6.1.4.1.29690.1.3.1 (AKA iso.org.dod.internet.privat

#define DrWeb_Admin_OID            DrWeb_AdminAttrs_OID
#define DrWeb_AdminReadOnly_OID    DrWeb_AdminAttrs_OID
#define DrWeb_AdminGroupOnly_OID   DrWeb_AdminAttrs_OID
#define DrWeb_AdminGroup_OID       DrWeb_AdminAttrs_OID
#define DrWeb_Admin_AttrName               "DrWebAdmin"
#define DrWeb_AdminReadOnly_AttrName      "DrWebAdminReadOnl
#define DrWeb_AdminGroupOnly_AttrName     "DrWebAdminGroupOr
#define DrWeb_AdminGroup_AttrName         "DrWebAdminGroup"
```

Le proprietà degli utenti Active Directory possono essere modificate manualmente sul server Active Directory (v. Autenticazione di

amministratori).

***Algoritmo di analisi degli attributi durante l'autorizzazione:***

1. Vengono letti gli attributi dell'utente.
2. Se il valore dell'attributo `DrWebAdmin` è `TRUE`:
   2.1. Se mancano alcuni attributi e il valore dell'attributo `DrWebInheritPermissions` è `TRUE`, gli attributi mancanti vengono letti dai gruppi. Appena tutti gli attributi sono stati impostati, la procedura di lettura dei gruppi termina. Così, gli attributi letti per primi hanno priorità più alta. Viene consentito l'accesso all'amministratore.
   2.2. Se mancano alcuni attributi e il valore dell'attributo `DrWebInheritPermissions` è `FALSE` (oppure il valore non è impostato), all'amministratore viene consentito l'accesso.
   2.3. Se tutti gli attributi sono impostati, all'amministratore viene consentito l'accesso.
3. Se il valore dell'attributo `DrWebAdmin` è `FALSE`, all'amministratore viene proibito l'accesso.
4. Se il valore dell'attributo `DrWebAdmin` non è impostato:
   4.1. Se l'attributo `DrWebInheritPermissions` assume il valore `TRUE`, gli attributi vengono letti dai gruppi. La procedura è come al passo 2.
   4.2. Se l'attributo `DrWebInheritPermissions` assume il valore `FALSE` (oppure il valore non è impostato), la procedura è come al passo 3.

## Autenticazione se si usa LDAP

Le impostazioni sono riportate nel file di configurazione `auth-ldap.xml`.

I tag principali del file di configurazione sono:

- `<enabled/>` e `<order/>` - sono simili alla variante per Active Directory.
- `<server/>` imposta l'indirizzo del server LDAP.

- <user-dn/> determina le regole di traduzione dei nomi in DN con l'impiego di maschere analoghe a maschere DOS.

  Nel tag <user-dn/> è consentito l'utilizzo di caratteri jolly:

  - * sostituisce con se una sequenza di caratteri ad eccezione di . , = @ \ e spazi;
  - # sostituisce con se una sequenza di caratteri.

- <user-dn-expr/> determina le regole di traduzione dei nomi in DN con l'impiego di espressioni regolari.

  Per esempio, questa è la stessa regola in diverse varianti:

  ```
  <user-dn          user="*@example.com"          dn="CN=
  \1,DC=example,DC=com"/>
  <user-dn-expr      user="(.*)@example.com"      dn="CN=
  \1,DC=example,DC=com"/>
  ```

  \1 .. \9 determina il posto per mettere nel pattern i valori *, # o espressioni tra parentesi.

  Secondo questo principio: se lo username è scritto come login@example.com, dopo la traduzione risulta DN: "CN=login,DC=example,DC=com".

- <user-dn-extension-enabled/> permette di eseguire lo script Lua ldap-user-dn-translate.ds (dalla cartella extensions) per tradurre lo username in DN. Questo script viene eseguito dopo aver cercato di usare tutte le regole user-dn, user-dn-expr in caso se non è stata trovata una regola appropriata. Lo script ha un parametro che è lo username che è stato immesso. Lo script restituisce una stringa che contiene DN oppure non contiene niente. In caso se non è stata trovata una regola appropriata e lo script non è consentito oppure non ha restituito niente, lo username immesso viene usato così com'è.
- Gli attributi dell'oggetto LDAP per il DN ottenuto come risultato di traduzione e i loro possibili valori possono essere ridefiniti dai tag (sono indicati i valori di default):

```
<!-- DrWebAdmin attribute equivalent (OID 1.3.6.1.4.
<admin-attribute-name value="DrWebAdmin" true-value=

<!-- DrWebAdminGroupOnly attribute equivalent (OID 1
<readonly-admin-attribute-name value="DrWebAdminRead

<!-- DrWebAdminGroupOnly attribute equivalent (OID 1
<grouponly-admin-attribute-name value="DrWebAdminGro

<!-- DrWebAdminGroup attribute equivalent (OID 1.3.6
<groups-admin-attribute-name value="DrWebAdminGroup"
```

Come valori di parametri `true-value`/`false-value` vengono impostati espressioni regolari.

- Se sono rimasti alcuni valori degli attributi dell'amministratore che non sono stati definiti, in caso se nel file di configurazione si imposta il tag `<group-reference-attribute-name value="memberOf"/>`, il valore dell'attributo memberOf si considera come una lista dei gruppi DN in cui rientra il dato amministratore, e gli attributi richiesti vengono cercati in questi gruppi così come nel caso quando si usa Active Directory.

# Allegato P. Licenze

In questa sezione è riportata una lista delle librerie di software di terze parti utilizzate dal software **Dr.Web ESS** e anche sono disponibili le informazioni sulle licenze e gli indirizzi dei progetti.

| Libreria di terze parti | Licenza | URL del progetto |
|---|---|---|
| boost | http://www.boost.org/users/license.html* | http://www.boost.org/ |
| c-ares | MIT License* | http://c-ares.haxx.se/ |
| Gecko SDK | Mozilla Public License*<br>GNU Lesser General Public License*<br>GNU General Public License* | https://developer.mozilla.org/ru/docs/Gecko_SDK |
| jQuery | MIT License*<br>GNU General Public License* | http://jquery.com/ |
| libcurl | http://curl.haxx.se/docs/copyright.html* | http://curl.haxx.se/libcurl/ |
| libradius | © Juniper Networks, Inc.* | http://www.freebsd.org |
| libxml2 | MIT License* | http://www.xmlsoft.org/ |
| lua | MIT License* | http://www.lua.org/ |
| lua-xmlreader | MIT License* | http://asbradbury.org/projects/lua-xmlreader/ |
| md5 implementation | © WIDE Project* | – |
| Net-snmp | http://www.net-snmp.org/about/license.html* | http://www.net-snmp.org/ |
| OpenLDAP | http://www.openldap.org/software/release/license.html* | http://www.openldap.org |
| OpenSSL | http://www.openssl.org/source/license.html* | http://www.openssl.org/ |

| Libreria di terze parti | Licenza | URL del progetto |
|---|---|---|
| Oracle Instant Client | http://www.oracle.com/technetwork/licenses/instant-client-lic-152016.html* | http://www.oracle.com |
| pcre | http://www.pcre.org/licence.txt* | http://www.pcre.org/ |
| Prototype JavaScript framework | MIT License* | http://prototypejs.org/assets/2009/8/31/prototype.js |
| Regina Rexx Interpreter | GNU Lesser General Public License* | http://regina-rexx.sourceforge.net/ |
| sha2 implementation | © Dr. Brian Gladman, Worcester, UK* | – |
| SQLite | Public Domain (http://www.sqlite.org/copyright.html) | http://www.sqlite.org/ |
| wtl | Common Public License (http://opensource.org/licenses/cpl1.0.php)* | http://sourceforge.net/projects/wtl/ |
| XML/SWF Charts | Bulk License (http://maani.us/xml_charts/index.php?menu=Buy) | http://www.maani.us/xml_charts/index.php?menu=Introduction |
| zlib | http://www.zlib.net/zlib_license.html* | http://www.zlib.net/ |

* - i testi delle licenze sono riportati più avanti.

## P1. Boost

```
Boost Software License - Version 1.0 - August 17th, 2003


Permission is hereby granted, free of charge, to any
person or organization obtaining a copy of the software
and accompanying documentation covered by this license
```

(the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

## P2. Curl

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2013, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

## P3. Libradius

Copyright 1998 Juniper Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR

CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

$FreeBSD: src/lib/libradius/radlib_private.h,v 1.6.30.3 2012/04/21 18:30:48 melifaro Exp $

## P4. MD5 implementation

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the project nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE PROJECT AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,

INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## P5. Net-snmp

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND

CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright (c) 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above

copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

```
*   Redistributions in binary form must reproduce the
above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other
materials provided with the distribution.


*   Neither the name of ScienceLogic, LLC nor the names
of its contributors may be used to endorse or promote
products derived from this software without specific
prior written permission.


THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL
THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT,   STRICT   LIABILITY,   OR   TORT   (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.
```

## P6. OpenLDAP

```
The OpenLDAP Public License

  Version 2.8, 17 August 2003


Redistribution and use of this software and associated
documentation     ("Software"),     with     or     without
modification, are permitted provided that the following
conditions are met:


1. Redistributions in source form must retain copyright
statements and notices,
```

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following

disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.

Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR (S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

```
OpenLDAP is a registered trademark of the OpenLDAP
Foundation.


Copyright 1999-2003 The OpenLDAP Foundation, Redwood
City,

California, USA.  All Rights Reserved.  Permission to
copy and

distribute verbatim copies of this document is granted.
```

## P7. OpenSSL

```
LICENSE ISSUES

  ==============


  The OpenSSL toolkit stays under a dual license, i.e.
both the conditions of the OpenSSL License and the
original SSLeay license apply to the toolkit.

  See below for the actual license texts. Actually both
licenses are BSD-style Open Source licenses. In case of
any license issues related to OpenSSL please contact
openssl-core@openssl.org.


  OpenSSL License

  ---------------


 ================================================

  Copyright (c) 1998-2011 The OpenSSL Project.  All
rights reserved.


  Redistribution and use in source and binary forms,
with or without modification, are permitted provided
that the following conditions are met:
```

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

=====

This product includes cryptographic software written by Eric Young

(eay@cryptsoft.com). This product includes software written by Tim

Hudson (tjh@cryptsoft.com).

Original SSLeay License

---

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

```
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.



  The licence and distribution terms for any publically
available version or derivative of this code cannot be
changed.  i.e. this code cannot simply be copied and put
under another distribution licence

  [including the GNU Public Licence.]
```

## P8. Oracle Instant Client

```
Export Controls on the Programs

Selecting the "Accept License Agreement" button is a
confirmation of your agreement that you comply, now and
during the trial term, with each of the following
statements:



-You are not a citizen, national, or resident of, and
are not under control of, the government of Cuba, Iran,
Sudan, Libya, North Korea, Syria, nor any country to
which the United States has prohibited export.

-You will not download or otherwise export or re-export
the Programs, directly or indirectly, to the above
mentioned countries nor to citizens, nationals or
residents of those countries.

-You are not listed on the United States Department of
Treasury lists of Specially Designated Nationals,
Specially Designated Terrorists, and Specially
Designated Narcotic Traffickers, nor are you listed on
the United States Department of Commerce Table of Denial
Orders.



You will not download or otherwise export or re-export
the Programs, directly or indirectly, to persons on the
above mentioned lists.



You will not use the Programs for, and will not allow
```

the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS

You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle®'s Global Trade Compliance web site (http://www.oracle.com/products/export).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable multilateral law, failure to comply with this policy could result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN License Agreement terms also apply to all updates you receive under your Technology Track subscription.

The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology Track software CDs and previous OTN License terms (including the Oracle Program License as modified by the OTN Program Use Certificate).

Oracle Technology Network Development and Distribution License Agreement for Instant Client

"We," "us," and "our" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that wishes to use the Programs from Oracle under this Agreement. "Programs" refers to the Software Products referenced below that you wish to download and use and Program documentation. "License" refers to your right to use the Programs and Program documentation under the terms of this Agreement. The substantive and procedural laws of California govern this Agreement. You and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco, San Mateo, or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

We are willing to license the Programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and select the "Accept" button at the bottom of the page to confirm your acceptance. If you are not willing to be bound by these terms, select the "Do Not Accept" button and the registration process will not continue.

Software Product

- Instant Client

License Rights

License.

We grant you a non-exclusive right and license to use the Programs solely for your business purposes and development and testing purposes, subject to the terms of this Agreement. You may allow third parties to use the Programs, subject to the terms of this Agreement, provided such third party use is for your business operations only.

Distribution License

We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the

Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information Transactions Act.

You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at http://www.oracle.com/technetwork/indexes/documentation/index.html.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions

We retain all ownership and intellectual property rights

in the Programs. You may make a sufficient number of copies of the Programs for the licensed use and one copy of the Programs for backup purposes.

You may not:

-use the Programs for any purpose other than as provided above;

-charge your end users for use of the Programs;

-remove or modify any Program markings or any notice of our proprietary rights;

-assign this agreement or give the Programs, Program access or an interest in the Programs to any individual or entity except as provided under this agreement;

-cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs;

-disclose results of any Program benchmark tests without our prior consent.

Export

You agree that U.S. export control laws and other applicable export and import laws govern your use of the Programs, including technical data; additional information can be found on Oracle's Global Trade Compliance web site located at http://www.oracle.com/products/export/index.html. You agree that neither the Programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support

Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply

with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.

Relationship Between the Parties

The relationship between you and us is that of licensee/ licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this Agreement is the complete agreement for the Programs and licenses, and this Agreement supersedes all prior or contemporaneous Agreements or representations. If any term of this Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective.

Last updated: 01/24/08

Should you have any questions concerning this License Agreement, or if you desire to contact Oracle for any reason, please write:

Oracle America, Inc.

500 Oracle Parkway,

Redwood City, CA 94065

Oracle may contact you to ask if you had a satisfactory experience installing and using this OTN software download.

## P9. PCRE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

The basic library functions are written in C and are freestanding. Also included in the distribution is a set of C++ wrapper functions, and a just-in-time compiler that can be used to optimize pattern matching. These are

```
both optional features that can be omitted when the
library is built.


THE BASIC LIBRARY FUNCTIONS

---------------------------


Written by:       Philip Hazel

Email local part: ph10

Email domain:     cam.ac.uk


University of Cambridge Computing Service,

Cambridge, England.


Copyright (c) 1997-2013 University of Cambridge

All rights reserved.


PCRE JUST-IN-TIME COMPILATION SUPPORT

-------------------------------------


Written by:       Zoltan Herczeg

Email local part: hzmester

Emain domain:     freemail.hu


Copyright(c) 2010-2013 Zoltan Herczeg

All rights reserved.


STACK-LESS JUST-IN-TIME COMPILER

--------------------------------
```

```
Written by:        Zoltan Herczeg

Email local part: hzmester

Emain domain:      freemail.hu


Copyright(c) 2009-2013 Zoltan Herczeg

All rights reserved.


THE C++ WRAPPER FUNCTIONS

-------------------------


Contributed by:   Google Inc.


Copyright (c) 2007-2012, Google Inc.

All rights reserved.


THE "BSD" LICENCE

-----------------


Redistribution and use in source and binary forms, with
or without modification, are permitted provided that the
following conditions are met:


     * Redistributions of source code must retain the
above copyright notice, this list of conditions and the
following disclaimer.


    * Redistributions in binary form must reproduce the
above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other
materials provided with the distribution.
```

```
     * Neither the name of the University of Cambridge
nor the name of Google Inc. nor the names of their
contributors may be used to endorse or promote products
derived from this software without specific prior
written permission.


THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.
```

## P10. Sha2 implementation

```
        Copyright (c) 2001, Dr Brian Gladman
<brg@gladman.me.uk>, Worcester, UK.

   All rights reserved.


   TERMS


    Redistribution and use in source and binary forms,
with or without modification, are permitted subject to
the following conditions:


    1. Redistributions of source code must retain the
above copyright notice, this list of conditions and the
following disclaimer.
```

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission.

This software is provided 'as is' with no express or implied warranties of correctness or fitness for purpose.

---

This is a byte oriented version of SHA256 that operates on arrays of bytes stored in memory. The operation uses a type 'sha256_ctx' to hold details of the current hash state and uses the following three calls:

void sha256_begin(sha256_ctx ctx[])

void sha256_hash(const unsigned char data[], unsigned long len, sha256_ctx ctx[])

void sha256_end(unsigned char hval[], sha256_ctx ctx[])

The first subroutine initialises a hash computation by setting up the context in the sha256_ctx context.

The second subroutine hashes 8-bit bytes from array data[] into the hash state withinh sha256_ctx context, the number of bytes to be hashed being given by the the unsigned long integer len.

The third subroutine completes the hash calculation and places the resulting digest value in the array of 8-bit bytes hval[]

```
    This implementation of SHA256 also supports SHA384
and SHA512 but these hash functions depend on the use of
64-bit long integers and are not very efficient on 32-
bit machines. This code is NOT recommended for these
hash functions.


     My thanks to Erik Andersen <andersen@codepoet-
consulting.com> for testing this code on big-endian
systems and for his assistance with corrections
```

## P11. Wtl

```
Common Public License Version 1.0


THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF
THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE,
REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES
RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.


1. DEFINITIONS


"Contribution" means:


a) in the case of the initial Contributor, the initial
code and documentation distributed under this Agreement,
and


b) in the case of each subsequent Contributor:


i) changes to the Program, and


ii) additions to the Program;
```

where such changes and/or additions to the Program originate from and are distributed by that particular Contributor. A Contribution 'originates' from a Contributor if it was added to the Program by such Contributor itself or anyone acting on such Contributor's behalf. Contributions do not include additions to the Program which: (i) are separate modules of software distributed in conjunction with the Program under their own license agreement, and (ii) are not derivative works of the Program.

"Contributor" means any person or entity that distributes the Program.

"Licensed Patents " mean patent claims licensable by a Contributor which are necessarily infringed by the use or sale of its Contribution alone or when combined with the Program.

"Program" means the Contributions distributed in accordance with this Agreement.

"Recipient" means anyone who receives the Program under this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive,

worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form.

This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably

allows subsequent Recipients to identify the originator of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor ("Commercial Contributor") hereby agrees to defend and indemnify every other Contributor ("Indemnified Contributor") against any losses, damages and costs (collectively "Losses") arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement. In order to qualify, an Indemnified Contributor must: a) promptly notify the Commercial Contributor in writing of such claim, and b) allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense.

For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor's responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those

damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent (s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the

intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

## P12. Zlib

zlib.h -- interface of the 'zlib' general purpose compression library

version 1.2.8, April 28th, 2013

Copyright (C) 1995-2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly — jloup@gzip.org

Mark Adler — madler@alumni.caltech.edu

## P13. MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

# P14. GNU General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if

you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To

prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code

form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf,

under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to “keep intact all notices”.

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are

being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if

neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a

statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's “contributor version”.

A contributor's “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for

the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the

conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be

used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an

absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

END OF TERMS AND CONDITIONS

## P15. GNU Lesser General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

This version of the GNU Lesser General Public License incorporates the terms and conditions of version 3 of the GNU General Public License, supplemented by the additional permissions listed below.

0. Additional Definitions.

As used herein, “this License” refers to version 3 of the GNU Lesser General Public License, and the “GNU GPL” refers to version 3 of the GNU General Public License.

“The Library” refers to a covered work governed by this License, other than an Application or a Combined Work as defined below.

An “Application” is any work that makes use of an interface provided by the Library, but which is not otherwise based on the Library. Defining a subclass of a

class defined by the Library is deemed a mode of using an interface provided by the Library.

A “Combined Work” is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the “Linked Version”.

The “Minimal Corresponding Source” for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The “Corresponding Application Code” for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a

reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of

this License.

b) Give prominent notice with the combined library that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

6. Revised Versions of the GNU Lesser General Public License.

The Free Software Foundation may publish revised and/or new versions of the GNU Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library as you received it specifies that a certain numbered version of the GNU Lesser General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that published version or of any later version published by the Free Software Foundation. If the Library as you received it does not specify a version number of the GNU Lesser General Public License, you may choose any version of the GNU Lesser General Public License ever published by the Free Software Foundation.

If the Library as you received it specifies that a proxy can decide whether future versions of the GNU Lesser General Public License shall apply, that proxy's public statement of acceptance of any version is permanent authorization for you to choose that version for the Library.

## P16. Mozilla Public License

Version 2.0

1. Definitions

1.1. “Contributor”

means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.

1.2. “Contributor Version”

means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor’s Contribution.

1.3. “Contribution”

means Covered Software of a particular Contributor.

1.4. “Covered Software”

means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. “Incompatible With Secondary Licenses”

means

that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. “Executable Form”

means any form of the work other than Source Code Form.

1.7. “Larger Work”

means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. “License”

means this document.

1.9. “Licensable”

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. “Modifications”

means any of the following:

any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

any new file in Source Code Form that contains any Covered Software.

1.11. “Patent Claims” of a Contributor

means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made,

import, or transfer of either its Contributions or its Contributor Version.

1.12. “Secondary License”

means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. “Source Code Form”

means the form of the work preferred for making modifications.

1.14. “You” (or “Your”)

means an individual or a legal entity exercising rights under this License. For legal entities, “You” includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

for any code that a Contributor has removed from Covered Software; or

for infringements caused by: (i) Your and any other third party’s modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for,

warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an "as is" basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence

to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party’s ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B - “Incompatible With Secondary Licenses” Notice

This Source Code Form is “Incompatible With Secondary Licenses”, as defined by the Mozilla Public License, v. 2.0.

# FAQ

## Trasporto di Dr.Web Enterprise Server su altro computer (nel SO Windows®)

***Per trasportare Dr.Web Enterprise Server (durante l'installazione della versione analoga di Dr.Web Enterprise Server) nel SO Windows:***

1. Arrestare il servizio **Dr.Web Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).
2. Avviare dalla riga di comando il file `drwcsd.exe` con la chiave `exportdb` per esportare i contenuti del database nel file. Nella versione per SO Windows la riga di comando completa che definisce l'esportazione avrà l'aspetto simile a:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin
   \drwcsd.exe" exportdb <percorso_al_file>
   ```

3. Salvare i contenuti della cartella `C:\Program Files\DrWeb Enterprise Server\etc`, nonché la chiave `drwcsd.pub` da `C:\Program Files\DrWeb Enterprise Server\Installer`.
4. Eliminare il **Server**.
5. Installare un **Server** nuovo (vuoto, con un database nuovo) sul computer richiesto. Arrestare il servizio **Dr.Web Enterprise Server** con gli strumenti di gestione dei servizi del SO Windows o con il **Centro gestione**.
6. Copiare i contenuti della cartella `etc`, salvati in precedenza, nel `C:\Program Files\DrWeb Enterprise Server\etc`, nonché la chiave `drwcsd.pub` nel `C:\Program Files\DrWeb Enterprise Server\Installer`.
7. Avviare dalla riga di comando il file `drwcsd.exe` con la chiave `importdb` per importare i contenuti del database dal

file. La riga di comando completa per importare nella versione nel SO Windows avrà l'aspetto simile a:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" importdb <percorso_al_file>
```

8. Avviare il servizio **Dr.Web Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).



Utilizzando il database interno dei dati si può non eseguire l'esportazione e l'importazione del database, ma semplicemente salvare il file del database interno `dbinternal.dbs` e sostituire il nuovo file del database sul **Server** installato con il file precedente, conservato dal **Server** precedente.

***Per il trasporto di Dr.Web Enterprise Server (durante l'installazione di un'altra versione di Dr.Web Enterprise Server) nel SO Windows:***

1. Arrestare il servizio **Dr.Web Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).
2. Salvare il database con gli strumenti di SQL server (se si utilizza il database interno, salvare semplicemente il file `dbinternal.dbs`).
3. Salvare i contenuti della cartella `C:\Program Files\DrWeb Enterprise Server\etc`, nonché la chive `drwcsd.pub` dal `C:\Program Files\DrWeb Enterprise Server\Installer`.
4. Eliminare il **Server**.
5. Installare un **Server** nuovo (vuoto, con un database nuovo) sul computer richiesto. Arrestare il servizio **Dr.Web Enterprise Server** con gli strumenti di gestione dei servizi del SO Windows o con il **Centro gestione**.
6. Copiare i contenuti della cartella `etc`, salvati in precedenza, nel `C:\Program Files\DrWeb Enterprise Server\etc`, nonché la chiave `drwcsd.pub` nel `C:\Program Files\DrWeb Enterprise Server\Installer`.

7. Ripristinare il database sul nuovo **Server**, indicare nel file di configurazione `drwcsd.conf` il percorso al database.
8. Avviare dalla riga di comando il file `drwcsd.exe` con la chiave `upgradedb` per aggiornare il database. La riga di comando completa per importare nelle versioni nel SO Windows avrà questo aspetto:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" upgradedb "C:\Program Files
\DrWeb Enterprise Server\update-db"
```

9. Avviare il servizio **Dr.Web Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).

***Se durante il trasporto si cambia l'indirizzo IP del Server:***

1. Trasportare il **Server** secondo la procedura corrispondente descritta sopra.
2. Definire l'indirizzo del nuovo **Server** nelle impostazioni di tutti gli **Agent** che sono stati serviti dal **Server** che viene trasportato (v. Connessione di Agent Dr.Web Enterprise Agent ad un altro Dr.Web Enterprise Server).
3. Perché al nuovo **Server** possano connettersi gli **Agent** per cui l'indirizzo del nuovo **Server** viene indicato tramite **Centro gestione** e non nelle impostazioni dell'**Agent** stesso sulla postazione, lasciare accesi entrambi i **Server** (su entrambi i **Server** è necessario indicare nelle impostazioni dell'**Agent** l'indirizzo del nuovo **Server**) fino a quando tutti gli **Agent** si siano connessi al **Server** vecchio per ottenere il nuovo indirizzo IP e siano passati al **Server** nuovo.

# Connessione di Agent Dr.Web Enterprise Agent ad un altro Dr.Web Enterprise Server



Durante la connessione di **Agent** all'altro Server tutte le azioni su workstation si devono eseguire con i diritti dell'amministratore del SO.

***Per riconnettere Dr.Web Enterprise Agent ad un altro Dr.Web Enterprise Server si deve:***

1. Se la chiave di codifica aperta `drwcsd.pub` del nuovo **Server** non corrisponde alla chiave di codifica del **Server** precedente, se si deve sostituire tale chiave su **Agent**:
   1.1. Se sul computer con **Agent** è disattivata l'autoprotezione, si deve disattivare il componente **SelfPROtect** via le configurazioni di **Agent** (per farlo, sono necessari i diritti dell'amministratore su workstation e i diritti per disattivare l'autoprotezione, installati sul **Server)**.
   1.2. Copiare nella cartella di installazine di **Agent** la chiave aperta di codifica `drwcsd.pub` dal nuovo **Server**.
2. Modificare l'indirizzo del **Server** nelle impostazioni di **Agent**:
   - Via il **Centro gestione** (del **Server** precedente): voce **Rete antivirus** del menu principale → voce **Dr.Web Enterprise Agent per Windows** del menu di gestione → scheda **Rete** → campo **Server**.
   - Direttamente su workstation: con la voce del menu contestuale dell'**Agent** **Impostazioni** → **Connessione** → campo **Server**.
3. Passare workstation a nuove (ripristinare i parametri di connessione al **Server**):

- Via il **Centro gestione** (del **Server** nuovo): voce **Amministrazione** del menu principale → voce **Configurazione Dr.Web Enterprise Server** del menu di gestione → scheda **Generali** → mettere il flag **Trasferisci le postazioni non autorizzate in nuovi arrivi**.
- Direttamente su workstation: con la voce del menu contestuale dell'**Agent** **Impostazioni** → **Connessione** → tasto **Novizio**.

4. Riavviare **Agent** (v. Dr.Web Enterprise Agent).

***Se per workstation non sono impostati i diritti di modifica delle configurazioni di Dr.Web Enterprise Agent, utilizzare la seguente procedura:***

1. Se la chiave di codifica aperta `drwcsd.pub` del nuovo **Server** non corrisponde alla chiave di codifica del **Server** precedente, si deve sostituire tale chiave su **Agent**:
   1.1. Se su computer con **Agent** è disattivata l'autoprotezione, si deve disattivare il componente **SelfPROtect** via le configurazioni di **Agent** (per farlo, sono necessari i diritti dell'amministratore su workstation e i diritti di disattivare l'autoprotezione, installati sul **Server).**
   1.2. Copiare nella cartella di installazione di **Agent** la chiave aperta di codifica `drwcsd.pub` dal nuovo **Server**.
2. Impostare le configurazioni di **Agent** con il seguente comando:

   ```
   drwagntd -save <ip_nuovo_server>
   ```

   dove *<ip_nuovo_server>* - indirizzo del nuovo **Server**, al cui si deve connettere l'**Agent**. Indirizzo viene impostato nel formato di indirizzi di rete.
3. Riavviare l'**Agent** (v. Dr.Web Enterprise Agent).

# Cambio tipo DBMS di Dr.Web Enterprise Security Suite

## Per il SO Windows

1. Arrestare il servizio **Dr.Web Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).
2. Avviare il file `drwcsd.exe` con la chiave `exportdb` per esportare i contenuti del database nel file. La riga di comando completa per esportare nella versione nel SO Windows avrà l'aspetto, simile a:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin
   \drwcsd.exe" -home="C:\Program Files\DrWeb
   Enterprise Server" -var-root="C:\Program
   Files\DrWeb Enterprise Server\var" -
   verbosity=all exportdb D:\esbase.es
   ```

   In questo esempio si sottintende, che **Dr.Web Enterprise Server** è installato nella cartella `C:\Program Files\DrWeb Enterprise Server`, e il database viene esportato in un file `esbase.es` nella radice del disco `D`. Copiare questa riga (è una riga) via il Copyboard nel file `cmd` ed eseguirlo.

   Se nel percorso al file ci sono degli spazi e/o caratteri nazionali (o il nome del file contiene degli spazi e/o caratteri nazionali), il percorso al file deve essere indicato tra le virgolette: `"D:\`*<nome completo>*`\esbase.es"`.

3. Avviare il servizio **Dr.Web Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server), connettere ad esso il **Centro gestione** e reconfigurare il **Server** per utilizzare un altro DBMS. Rifiutare la proposta di riavviare il **Server**.
4. Arrestare il servizio **Dr.Web Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).
5. Avviare il file `drwcsd.exe` con la chiave `initdb` per

inizializzazione di un nuovo database. La riga di inizializzazione del database per la versione del **Server** nel SO Windows avrà l'aspetto, simile a:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program
Files\DrWeb Enterprise Server\var" -
verbosity=all initdb D:\Keys\agent.key - -
<password>
```

Si sottintende, che il **Server** è installato nella cartella `"C:\Program Files\DrWeb Enterprise Server"`, e la chiave di agent `agent.key` si trova nel `D:\Keys`. Copiare questa riga (è una riga) via il Copyboard nel file `cmd` ed eseguirlo.

Se nel percorso al file ci sono degli spazi e/o caratteri nazionali (o il nome del file contiene degli spazi e/o caratteri nazionali), il percorso al file deve essere indicato tra le virgolette: `"D:\`*<nome completo>*`\agent.key"`.

6. Avviare il file `drwcsd.exe` con la chiave `importdb` per importare i contenuti del database dal file. La riga di comando completa per importare nella versione nei SO Windows avrà l'aspetto simile a:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program
Files\DrWeb Enterprise Server\var" -
verbosity=all importdb D:\esbase.es"
```

Copiare questa riga (è una riga) via il Copyboard nel file cmd ed eseguirlo.

7. Avviare il servizio **Dr.Web Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).

## Per i SO della famiglia UNIX

1. Arrestare il servizio **Dr.Web Enterprise Server** con lo script:
   - per i SO **Linux** e **Solaris**:

     ```
     /etc/init.d/drwcsd stop
     ```

   - per il SO **FreeBSD**:

     ```
     /usr/local/etc/rc.d/drwcsd.sh stop
     ```

   o con il **Centro gestione** (oltre i SO Solaris).

2. Avviare il **Server** con la chiave `exportdb` per esportare i contenuti del database nel file. La riga di comando della cartella di installazione del **Server** avrà l'aspetto, simile a:
   - per il SO **Linux**:

     ```
     "/etc/init.d/drwcsd exportdb /var/opt/
     drwcs/esbase.es"
     ```

   - per il SO **Solaris**:

     ```
     "/etc/init.d/drwcsd exportdb /var/drwcs/
     etc/esbase.es"
     ```

   - per il SO **FreeBSD**:

     ```
     "/usr/local/etc/rc.d/drwcsd.sh exportdb /
     var/drwcs/esbase.es"
     ```

   In questo esempio si sottintende, che il database viene esportato nel file `esbase.es`, locato nella cartella di utente.

3. Avviare il servizio **Dr.Web Enterprise Server** con lo script:
   - per i SO **Linux** e **Solaris**:

     ```
     /etc/init.d/drwcsd start
     ```

   - per il SO **FreeBSD**:

     ```
     /usr/local/etc/rc.d/drwcsd.sh start
     ```

   Connettere il **Centro gestione** e reconfigurare il **Server** per

utilizzare un altro DBMS: nel menu **Amministrazione** → voce **Configurazione Dr.Web Enterprise Server** → scheda **Base di dati**.



Cambio della configurazione del **Server** per utilizzare un altro DBMS può essere fatto, modificando direttamente il file di configurazione del **Server** `drwcsd.conf`. Per farlo, si deve passare ai commenti / eliminare il record del database attuale e definire un nuovo database (per più informazioni v. Allegato G1. File di configurazione di Dr.Web Enterprise Server).

Rifiutare la proposta di riavviare il **Server**.

4. Arrestare **Dr.Web Enterprise Server** (v. passo **1**).
5. Avviare il file `drwcsd` con la chiave `initdb` per inizializzazione di un database nuovo. La riga di inizializzazione avrà l'aspetto, simile a:
   - per i SO **Linux** e **Solaris**:

     ```
     /etc/init.d/drwcsd initdb
     ```

   - per il SO **FreeBSD**:

     ```
     /usr/local/etc/rc.d/drwcsd.sh initdb
     ```

6. Avviare il file `drwcsd` con la chiave `importdb` per importare i contenuti del database dal file. La riga di comando per l'importazione avrà l'aspetto, simile a:
   - per il SO **Linux**:

     ```
     "/etc/init.d/drwcsd importdb /var/opt/
     drwcs/esbase.es"
     ```

   - per il SO **Solaris**:

     ```
     "/etc/init.d/drwcsd importdb /var/drwcs/
     etc/esbase.es"
     ```

   - per il SO **FreeBSD**:

     ```
     "/usr/local/etc/rc.d/drwcsd.sh importdb /
     var/drwcs/esbase.es"
     ```

7. Avviare **Dr.Web Enterprise Server** (v. passo **3**).



Se all'avvio di script del **Server** si devono impostare i parametri (per esempio, indicare la cartella di installazione del **Server**, modificare il livello di dettagli di log ecc), la modifica dei valori corrispondenti viene eseguita nello script iniziale:

- per il SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh
```

- per i SO **Linux** e **Solaris**:

```
/etc/init.d/drwcsd
```

# Ripristino del database di Dr.Web Enterprise Security Suite

Durante l'operazione **Enterprise Server** regolarmente esegue il backup delle informazioni importanti (contenuti del database, file della chiave di licenza del **Server**, chiave di codifica chiusa, file di configurazione del **Server** e del **Centro gestione**). I backup si salvano nei seguenti cartelle rispetto alla cartella operativa del **Server**:

- per il SO **Windows**: `\var\Backup`
- per il SO **Linux**: `/var/opt/drwcs/backup`
- per i SO **FreeBSD** e **Solaris**: `/var/drwcs/backup`

Per farlo, nell'orario del **Server** è incluso il processo giornaliero, che esegue questa funzione. Se questo processo è assente dall'orario, si consiglia di crearlo.

I backup si salvano nel formato `.dz`, compatibile con `gzip` e con altri archiviatori. Dopo la decompressione tutti i file, oltre i contenuti del database, si possono utilizzare. I contenuti del database, salvati nel backup, si possono importare nel database operativo del **Server** con la chiave `importdb` e in questo modo ripristinare i dati.

## Ripristino del database per varie versioni di Dr.Web Enterprise Server

Si può ripristinare il database solo dalla copia di riserva, creata con il **Server** con la stessa versione maggiore della versione del **Server**, su cui avviene il ripristino.

**Per esempio:**

- il database dalla copia di riserva, creata con il **Server** della versione **5.0** si può ripristinare solo con il **Server** della versione **5.0**.
- il database dalla copia di riserva, creata con il **Server** della versione **6.0** si può ripristinare solo con il **Server** della versione

**6.0**.

- il database dalla copia di riserva, creata con il **Server** della versione **5.0** o **4.XX** non si possono ripristinare con il **Server** della versione **6.0**.

***Se durante l'aggiornamento del Server alla versione 6.0 dalle versioni precedenti per qualche raggione si sia danneggiato il database, eseguire il seguente:***

1. Eliminare il **Server** della versione **6.0**. In questo caso verranno automaticamente salvati le copie di riserva dei file, utilizzati dal **Server**.
2. Installare il **Server** della versione precedente al ripristino e con il quale è stato creato il backup.

   In questo caso, secondo la procedura standard di aggiornamento, si devono utilizzare tutti i file salvati del **Server** oltre il file del database.

   Durante l'installazione del **Server** creare un database nuovo.
3. Ripristinare il database dalla copia di riserva secondo le regole generali (v. sotto).
4. Nelle impostazioni del **Server** disattivare i protocolli di **Agent**, del **Server** e di **Installazione di rete**. Per farlo, scegliere la voce **Amministrazione** del menu principale del **Centro gestione**, nella finestra aperta scegliere la voce del menu di gestione **Configurazione Dr.Web Enterprise Server**, passare alla scheda **Moduli** e togliere i seguenti flag.
5. Aggiornare il **Server** alla versione **6.0** secondo le regole generali (v. Aggiornamento di Dr.Web Enterprise Security Suite e di suoi componenti singoli).
6. Attivare i protocolli di **Agent**, del **Server** e di **Installazione di rete**, disattivati al passo 4.

## Per il SO Windows

***Per ripristinare il database dalla copia di riserva:***

1. Arrestare il servizio di **Enterprise Server** (se è avviata, v. Avvio e arresto di Dr.Web Enterprise Server).

2. Importare dal file corrispondente del backup i contenuti del database. La riga di impostazione ha l'aspetto, simile a:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program
Files\DrWeb Enterprise Server\var" -
verbosity=all importdb "<disco:>
\<percorso_al_file_di_backup>\database.dz"
```

   Questo comando deve essere inserito in una riga sola. Si sottindende nell'esempio che il **Server** è installato nella cartella `C:\Program Files\DrWeb Enterprise Server`.

3. Avviare il servizio **Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).

***Per ripristinare il database dal backup al cambio della versione di Enterprise Server (nel quadro di una versione maggiore) o se si rovina la versione attuale del database:***

1. Arrestare il servizio di **Enterprise Server** (se è avviata, v. Avvio e arresto di Dr.Web Enterprise Server).
2. Eliminare i contenuti del database attuale. Per farlo:

   2.1. Se si utilizza il database interno:

   a) Eliminare il file del database `dbinternal.dbs`.

   b) Eseguire l'inizializzazione di un nuovo database. La riga di inizializzazione del database nella versione del **Server** nel SO Windows avrà l'aspetto, simile a:

```
"C:\Program Files\DrWeb Enterprise Server
\bin\drwcsd.exe" -home="C:\Program Files
\DrWeb Enterprise Server" -var-
root="C:\Program Files\DrWeb Enterprise
Server\var" -verbosity=all initdb D:\Keys
\agent.key - - <password>
```

   Questo comando deve essere inserito in una riga sola (v. anche il formato del comando `drwcsd` con la chiave `initdb` in Allegato. H5.3). Si sottindende nell'esempio che il **Server** è installato nella cartella `C:\Program Files\DrWeb`

`Enterprise Server`, e la chiave di agent `agent.key` si trova nella cartella `D:\Keys`.

c) Dopo l'esecuzione di questo comando nella cartella `var` della cartella di installazione di **Enterprise Server** si deve apparire un nuovo file del database `dbinternal.dbs` della dimensione circa 200 kB.

2.2. Se si utilizza il database esterno: eseguire la pulizia del database con lo script `clean.sql`, che si trova nella cartella `etc` della cartella di installazione del **Server**.

3. Importare dal file corrispondente del backup i contenuti del database. La riga di importazione ha il seguente aspetto:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" -home="C:\Program Files\DrWeb
Enterprise Server" -var-root="C:\Program
Files\DrWeb Enterprise Server\var" -
verbosity=all importdb "<disco:>
\<percorso_al_file_di_backup>\database.dz"
```

Questo comando deve essere inserito in una riga sola. Si sottintende nell'esempio che il **Server** è installato nella cartella `C:\Program Files\DrWeb Enterprise Server`.

4. Avviare il servizio di **Enterprise Server** (v. Avvio e arresto di Dr.Web Enterprise Server).

## Per i SO della famiglia UNIX

1. Arrestare **Enterprise Server** (se è avviato):
   - per i SO **Linux** e **Solaris**:

```
/etc/init.d/drwcsd stop
```

   - per il SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh stop
```

   - per **altre** versioni supportate:

```
/bin/drwcs.sh stop
```

2. Eliminare il file del database `dbinternal.dbs` dalla seguente directory della cartella di installazione di **Enterprise Server**:
   - per il SO **Linux**: `/var/opt/drwcs/`
   - per i SO **FreeBSD** e **Solaris**: `/var/drwcs/`



Se si utilizza il database esterno, la sua pulizia viene eseguita con lo script `clean.sql`, che si trova nella cartella:
- nel SO **Linux**: `/var/opt/drwcs/etc`
- nei SO **Solaris** e **FreeBSD**: `/var/drwcs/etc`

3. Inizializzare il database del **Server**. Per farlo, si utilizza il seguente comando:
   - per i SO **Linux** e **Solaris**:

```
/etc/init.d/drwcsd initdb
```

   - per il SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh initdb
```

   - per **altre** versioni supportate:

```
su drwcs -c "bin/drwcsd -var-root=./var -verbosity=all -log=./var/server.log initdb etc/agent.key - - <password>"
```

4. Dopo l'esecuzione di questo comando nella cartella `var` della cartella di installazione di **Enterprise Server** deve apparire un nuovo file del database `dbinternal.dbs` della dimensione circa di 200 kB.
5. Importare dal file corrispondente del backup i contenuti del database. La riga di importazione ha un aspetto, simile a:
   - per i SO **Linux** e **Solaris**:

```
/etc/init.d/drwcsd importdb "/<percorso_al_file_di_backup>/database.dz"
```

   - per il SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh importdb "/
```

```
<percorso_al_file_di_bakcup>/database.dz"
```

- per **altre** versioni supportate:

```
bin/drwcsd -var-root=./var -verbosity=all -
log=logfile.log importdb "/
<percorso_al_file_di_backup>/database.dz"
```

6. Avviare **Enterprise Server**.
   - per i SO **Linux** e **Solaris**:

```
/etc/init.d/drwcsd start
```

   - per il SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh start
```

   - per **altre** versioni supportate:

```
/bin/drwcs.sh start
```



Se all'avvio dello script del **Server** si devono impostare i parametri (per esempio, indicare la cartella di installazione del **Server**, modificare il livello di dettagli del log ecc), la modifica dei valori corrispondenti viene eseguita nello script iniziale:

- per il SO **FreeBSD**: `/usr/local/etc/rc.d/drwcsd.sh`
- per i SO **Linux** e **Solaris**: `/etc/init.d/drwcsd`

Se qualche **Agent** è stato installato dopo la creazione dell'ultimo backup ed è assente dal database dopo il ripristino, si consiglia di attivare l'opzione **Trasferisci le postazioni non autorizzate in nuovi arrivi**. Per farlo, nel **Centro gestione** nel menu **Amministrazione** scegliere la voce **Configurazione Dr.Web Enterprise Server**. Nella scheda **Generali** mettere il flag corrispondente.

Dopo il ripristino del database si consiglia di connettersi al **Server** via il **Centro gestione**, aprire nel menu **Amministrazione** la voce **Orario Dr.Web Enterprise Server** e controllare lì se c'è il processo **Copie di riserva dei dati critici del server.** Se non c'è questo processo, si consiglia di crearlo.

# Ripristino di Dr.Web Enterprise Server dal backup dei dati

**Dr.Web Enterprise Security Suite** salva regolarmente il backup delle informazioni importanti del **Server**: chiave di licenza del **Server**, contenuti del database, chiave di codifica, configurazione del **Server** e del **Centro gestione**. I backup vengono salvati nelle seguenti cartelle rispetto alla cartella operativa del **Server**:

- per i SO **Windows**: `\var\Backup`
- per i SO **Linux**: `/var/opt/drwcs/backup`
- per i SO **FreeBSD** e **Solaris**: `/var/drwcs/backup`

Per eseguire questa funzionalità, nell'orario del **Server** è incluso il processo giornaliero. Se questo processo è assente dall'orario, si consiglia di crearlo.

Le copie di riserva si salvano nel formato `.dz`, compatibile con `gzip` e con altri decompressori. Dopo la decompressione tutti i file, oltre i contenuti del database, si possono utilizzare. I contenuti del database, salvati nel backup, si possono importare in un'altro database del **Server** con la chiave `importdb` e in questo modo ripristinare i dati (v. Ripristino del database di Dr.Web Enterprise Security Suite).

Si consiglia inoltre di salvare su altra workstation i backup dei seguenti file: chiave di codifica `drwcsd.pri` e `drwcsd.pub`, chiavi di licenza `enterprise.key` e `agent.key`, certificato per SSL `certificate.pem`, chiave chiusa RSA `private-key.pem` e periodicamente salvare lì i backup dei contenuti del database del **Server** `database.dz`, file di configurazione del **Server** `drwcsd.conf` e il **Centro gestione** `webmin.conf`. In questo modo si può evitare la perdita dei dati al danneggiamento del computer, su cui è installato **Enterprise Server** e completamente ripristinare i dati e la funzionalità del **Server**. Se si perdono le chiavi di licenza, si possono richiedere di nuovo, come indicato in v. File della chiave.

## Per ripristinare Dr.Web Enterprise Server nei SO Windows

Su workstation installare il software di **Enterprise Server** della versione uguale a quella persa (v. Installazione di Dr.Web Enterprise Server per i SO Windows®). In questo caso:

- Se è salvato il backup del database (interno o esterno) su altro computer e non è stato danneggiato, indicare esso nella finestra di dialogo corrispondente di installazione, nonché i file salvati della chiave di licenza del **Server**, chiave di codifica chiusa e configurazione del **Server**.
- Se il database del **Server** (interno o esterno) è stato perso, ma è conservato il backup dei suoi contenuti `database.dz`, durante l'installazione nelle finestre di dialogo corrispondenti scegliere la creazione di un nuovo database, indicare i file salvati della chiave di licenza di **Server** e di **Agent**, chiave di codifica chiusa e configurazione del **Server**. Dopo l'installazione importare i contenuti del database dal backup (v. Ripristino del database di Dr.Web Enterprise Security Suite).

## Per ripristinare Dr.Web Enterprise Server nei SO della famiglia UNIX

1. Su workstation operativa installare il software di **Enterprise Server** della stessa versione di quella persa (v. Installazione di Dr.Web Enterprise Server nei SO della famiglia UNIX®).
2. Mettere i file salvati
   - per il SO **Linux**: nella cartella `/var/opt/drwcs/etc`, oltre la chiave `pub` da mettere in `/opt/drwcs/Installer/`
   - per il SO **FreeBSD**: nella cartella `/var/drwcs/etc`, oltre la chiave `pub` da mettere in `/usr/local/drwcs/Installer/`
   - per il SO **Solaris**: nella cartella `/var/drwcs/etc`, oltre la chiave `pub` da mettere in `/opt/drwcs/Installer/`



Su tutti i file sostituiti del **Server** si devono installare stessi diritti di sistema di quelli scelti all'installazione precedente (persa) del **Server**.

3. Generare un nuovo certificato SSL:
   - per i SO **Linux** e **Solaris**:

     ```
     /etc/init.d/drwcsd selfcert
     ```

   - per il SO **FreeBSD**:

     ```
     /usr/local/etc/rc.d/drwcsd.sh selfcert
     ```

   - per **altre** versioni supportate:

     ```
     /opt/drwcs/bin/drwcsd  -var-root=/var/drwcs
     -log=/var/drwcs/log/drwcsd.log selfcert
     ```

4. Le seguenti azioni dipendono dalla presenza del database del **Server**:

   a) Se c'è il database esterno del server, non si devono eseguire le azioni supplementari del ripristino a condizione che si sia salvato il file di configurazione e il build del **Server** corrisponda a quello precedente. Nel caso contrario si deve definire il database nel file di configurazione del **Server** e/o aggiornare la struttura del database con la chiave `upgradedb` (v. variante **c)** sottostante).

   b) Se c'è il backup del database `database.dz`, sia interno, sia esterno, avviare il **Server**, eliminare il database interno, creato durante installazione, inizializzare la creazione di un database nuovo ed importare i contenuti del database precedente dal backup (v. Ripristino del database di Dr.Web Enterprise Security Suite).

   c) Se c'è il file salvato del database interno, sostituire con esso il file nuovo:

   - per il SO **Linux**:
     `/var/opt/drwcs/dbinternal.dbs`
   - per i SO **FreeBSD** e **Solaris**:

```
/var/drwcs/dbinternal.dbs
```



Su tutti i file sostituiti del **Server** si devono installare i diritti di sistema, uguali a quelli scelti all'installazione precedente (persa) del **Server**.

Eseguire i comandi:

- per i SO **Linux** e **Solaris**:

```
/etc/init.d/drwcsd upgradedb
```

- per il SO **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd.sh upgradedb
```

- per **altre** versioni supportate:

```
/opt/drwcs/bin/drwcsd  -var-root=/var/drwcs
-log=/var/drwcs/log/drwcsd.log    upgradedb
update-db
```

5. Riavviare il **Server**.



Se qualche **Agent** è stato installato dopo la creazione dell'ultimo backup ed è assente dal database dopo il ripristino, si può passare la workstation alla modalità **Nuova** in remoto. Per farlo, si deve connettere il **Centro gestione** al **Server**, aprire il menu **Amministrazione** → voce **Configurazione Dr.Web Enterprise Server** → scheda **Generali** ed attivare la modalità **Trasferisci le postazioni non autorizzate in nuovi arrivi**.

# Aggiornamento di Agent sui server LAN

Durante aggiornamento di **Agent**, installati sui server LAN, possono essere indesiderabili riavvii di workstation o arresti del software di rete, che opera su tali workstation.

Per evitare che workstation, che eseguono le funzionalità importanti di LAN, siano funzionalmente ferme, si propone la modalità seguente di aggiornamento di **Agent** e del software antivirus:

1. Nell'orario del **Server** modificare i processi standard per aggiornare tutti i componenti ad aggiornamento solamente dei database dei virus.
2. Creare un processo nuovo dell'aggiornamento di tutti i componenti nel tempo comodo, quando non si potrà influire criticamente sull'operazione dei server LAN.

   Creazione e modifica dei processi nell'orario del **Server** sono riportate nella sezione Configurazione orario di Dr.Web Enterprise Server.



Sui server, che eseguono le funzionalità principali di rete (controller di dominio, server di distribuzione di licenze ecc), non si consiglia di installare i componenti **SpIDer Gate**, **SpIDer Mail** e **Dr.Web Firewall** per eventuare eventuali conflitti dei servizi di rete e dei componenti interni dell'antivirus **Dr.Web**.

# Ripristino della password di amministratore Dr.Web Enterprise Security Suite

In caso è stata persa la password di amministratore per accedere a **Enterprise Server**, esiste la possibilità di leggerla o modificarla utilizzando l'accesso diretto al database del **Server**:

a) Se si usa il database interno, per leggere e cambiare la password di amministratore viene utilizzata l'utilità `drwidbsh` che fa parte della distribuzione del **Server**.

b) Per il database esterno usare il client sql appropriato.



I parametri degli account di amministratori si memorizzano nella tabella `admins`.

### *Esempi di utilizzo dell'utilità drwidbsh*

1. Avviare l'utilità indicando il percorso al file del database:
   - In caso del database interno sotto SO Linux:

     ```
     /opt/drwcs/bin/drwidbsh     /var/opt/drwcs/
     dbinternal.dbs
     ```

   - In caso del database interno sotto SO Windows:

     ```
     "C:\Program Files\DrWeb Enterprise Server
     \bin\drwidbsh" "C:\Program Files\DrWeb
     Enterprise Server\var\dbinternal.dbs"
     ```

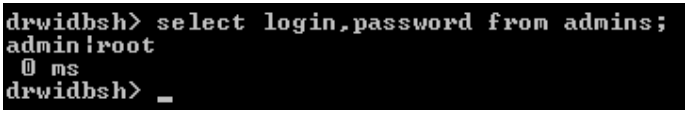
2. Per leggere tutti i dati memorizzati nella tabella `admins`, eseguire il comando:

   ```
   select * from admins;
   ```

3. Per leggere gli username e le password di tutti gli account di amministratori, eseguire il comando:

```
select login,password from admins;
```

4. La schermata sottostante mostra il risultato per la variante quando esiste solo un account con lo username `admin` e la password `root`:




5. Per modificare la password, usare il comando `update`. Il seguente è un esempio del comando che modifica la password dell'account `admin` su `qwerty`:

```
update admins set password='qwerty' where login='admin';
```

6. Per uscire dall'utilità, eseguire il comando:

```
.exit
```

Il funzionamento dell'utilità `drwidbsh` è descritto nell'allegato H6. Utilità di amministrazione del database incorporato.

# Utilizzo di DFS durante l'installazione di Agent via Active Directory

Durante installazione di **Enterprise Agent** via Active Directory si può utilizzare il servizio del file system distribuito (DFS).

Questo approccio potrebbe essere utile, per esempio, se nel LAN ci sono più controller di dominio.

***Durante installazione nella rete con più controller di dominio:***

1. Su ogni controller di dominio si può creare una cartella con lo stesso nome.
2. Con DFS unire le cartelle create in una cartella radice di destinazione.
3. Eseguire installazione amministrativa del pacchetto `*.msi` nella cartella di destinazione creata.
4. La cartella di destinazione ricevuta può essere utilizzata per assegnare il pacchetto nell'editor di oggetti della politica di gruppo.

   In questo caso si può utilizzare il nome di rete del genere: `\\<dominio>\<cartella>`

   dove: <*dominio*> - nome di dominio, <*cartella*> - nome di cartella di destinazione.

# Rilevamento dei problemi di installazione remota

***Principio di installazione:***

1. Il browser (plugin **Dr.Web Browser-Plugin**) si connette alla risorsa `ADMIN$` su workstation remota (`\\<workstation_remota>\ADMIN$`) e copia i file di installazione (`drwinst.exe`, `drwcsd.pub`), i percorsi ai quali sono indicati nel **Centro gestione**, nella cartella `\\<workstation_remota>\ADMIN$\Temp`.
2. Il plugin avvia il file `drwinst.exe` da eseguire su workstation remota con le chiavi, corrispondenti alle configurazioni nel **Centro gestione**.

***Per installazione con successo è necessario che su workstation, da cui viene eseguita installazione:***

1. Sia disponibile la risorsa `ADMIN$` su workstation remota.

   Si può verificare la disponibilità nel seguente modo:

   Inserire nella riga di indirizzo di applicazione `Windows Explorer`:

   `\\<workstation_remota>\ADMIN$`

   Deve apparire un invito di inserire utente e password per accedere a questa risorsa. Inserire i dati di utenza, che sono stati indicati nella pagina di installazione.

   La risorsa `ADMIN$` può essere non disponibile per seguenti cause:

   a) utenza non ha i diritti dell'amministratore;
   b) workstation è sconnessa o Firewall blocca accesso alla porta 445;

c) limitazioni di accesso remoto alla risorsa `ADMIN$` nel SO Windows Vista e superiori, se non fanno parte di dominio.

2. Ci sia accesso ai file `drwinst.exe` e `drwcsd.pub`.

Nel **Centro gestione** vengono visualizzate le informazioni avanzate (fase e codice errore), che permettono di rilevare la causa di errore.

## *Lista di errori più riscontrati*

| Fase | Codice errore | Causa |
|---|---|---|
| Verifica correttezza di indirizzi di workstation remote (1) | Questo host è sconosciuto (11001) | Non si è riusciti a trasformare il nome DNS di workstation in indirizzo. Questo nome DNS non esiste o è scorrettamente configurato il server di nomi. |
| Verifica disponibilità di risorse di rete su workstation remota (2) | È successo un errore di operazione su socket perché host finale è disattivato (10064) | Non è disponibile la porta TCP 445 su workstation remota, eventuali cause:<br>◆ workstation sconnessa;<br>◆ firewall blocca la porta indicata;<br>◆ su workstation è installato un SO, diverso dal SO Windows. |
| Connessione alla risorsa amministrativa `ADMIN$` (1001) | Su questa fase viene eseguita la connessione alla risorsa amministrativa `ADMIN$` su workstation remota. | |
| | Il sistema ha rilevato un possibile tentativo di compromissione della sicurezza. Verificare disponibilità di accesso al server, via cui è stato eseguito accesso (1265). | ◆ Non è configurato modello di accesso condiviso e di sicurezza per utenze locali.<br>◆ Non è disponibile server di autorizzazione (controller di dominio) |

| Fase | Codice errore | Causa |
|---|---|---|
| | Accesso al sistema non è eseguito: nome utente o password non riconosciuti (1326). | Utente sconosciuto o password scorretta. |
| | Errore di sintassi in nome di file, in nome di cartella o in volume label (123). | Non esiste la risorsa `ADMIN$` su workstation remota. |
| Verifica dello stato di completamento di operazione di installazione (1009) | Su questa fase viene eseguita la verifica del risultato di operazione di installazione. | |
| | Errore sconosciuto (2). | Rivolgersi al supporto tecnico della società **Doctor Web**. |
| | **Agent** è già installato, installazione non è richiesta (4). | Su questa workstation **Agent** è già installato o è stato eliminato scorrettamente (in questo caso utilizzare utilità **drwebremover**). |
| | Interruzione del protocollo (6). | Installazione (`drwinst.exe`) non corrisponde alla versione del **Server**. Assicurarsi che il programma di installazione è ottenuto dal kit di installazione del **Server**. |
| | Errore di inizializzazione REXX (7). | Errore di sistema. Rivolgersi al supporto tecnico della società **Doctor Web**. |
| | Timeout di connessione al **Server** (8). | **Enterprise Server** non è disponibile a workstation remota. |
| | Si deve riavviare il sistema per completare disinstallazione precedente (9). | Riavviare la workstation per completare il processo di disinstallazione precedente. |

# Indice analitico


## A

Active Directory
- eliminazione di agent 95
- installazione di agent 80

agent
- aggiornamento 303, 312
- avvio 107
- chiavi di avvio 397
- configurazione 200
- eliminazione 92, 95
- funzioni 103
- installazione 64
- installazione, Active Directory 80
- installazione, su remoto 73, 80
- interfaccia 103, 104
- modalità mobile 312

aggiornamenti
- rete antivirus 284

aggiornamento
- agent 303, 312
- chiavi 314
- Dr.Web Browser-Plugin 287
- Dr.Web ESS 287
- forzato 305
- limitazione 311
- manuale 305
- modalità mobile 312
- proxy 303
- repository 309
- secondo l'orario 307
- server, per SO UNIX 294
- server, per SO Windows 287

amministratori
- diritti 163
- utenze 164

autorizzazione
- automatica 125
- Centro gestione 125

avvio
- Dr.Web Enterprise Agent 107
- Dr.Web Enterprise Server 101

avvisi
- configurazione 261
- parametri 348
- parametri template 349

## B

backup
- DB (database) 530
- server antivirus 537

blocco
- risorse locali 239

## C

cartella di server, contenuti 45

Centro gestione
- barra degli strumenti 117
- barra delle proprietà 121

# Indice analitico


Centro gestione
- descrizione 107
- file di configurazione 384
- lista gerarchica 115
- menu principale 110
- pannello di ricerca 111

chiavi 29
- aggiornamento 314
- codifica, generazione 418
- demo 31
- ottenimento 29
- vedi anche registrazione 29

chiavi di avvio
- agent 397
- installazione di rete 400
- modulo interfaccia 395
- server antivirus 403

codifica
- chiavi, generazione 418
- traffico 256

componenti
- antivirali, composizione 189
- contenuti 17
- rete antivirus 143
- sincronizzazione 305

compressione traffico 256
configurazione 189, 200
- agent 200
- copiatura 183
- pacchetto antivirus 189
- postazione 189
- postazioni 189
- server antivirus 247

connessione workstation 186
console web
- creazione utenza 55

creazione
- gruppo 173
- record di workstation 55


## D


DB (database)
- backup 530
- configurazione 258
- DBMS 525
- incorporato 333
- Oracle 338
- PostgreSQL 345
- ripristino 530
- SQL CE 342

diritti
- amministratori 163

distribuzione 28
Dr.Web Browser-Plugin
- aggiornamento 302
- eliminazione 92
- eliminazione, per SO UNIX 97
- installazione 52

# Indice analitico


Dr.Web Enterprise Agent
- aggiornamento 303, 312
- avvio 107
- chiavi di avvio 397
- configurazione 200
- eliminazione 92, 95
- funzioni 103
- installazione 64
- installazione, Active Directory 80
- installazione, su remoto 73, 80
- interfaccia 103, 104
- modalità mobile 312

Dr.Web Enterprise Server
- aggiornamento, per SO UNIX 294
- aggiornamento, per SO Windows 287
- avvio 101
- chiavi di avvio 403
- configurazione 247
- contenuti di cartella 45
- eliminazione, per SO UNIX 95
- eliminazione, per SO Windows 92
- file di configurazione 375
- impostazione legami 276
- installazione, per SO UNIX 46
- installazione, per SO Windows 34
- interfaccia 101
- log 263
- orario 264
- protocollo 100
- ripristino 537
- task 99
- tipi di legami 273
- trasporto 520

## E

editor template 262

eliminazione
- agent 92
- agent, Active Directory 95
- componenti 92
- componenti antivirus 189
- Dr.Web Browser-Plugin 92, 97
- gruppi 174
- pacchetto antivirus 92
- postazione, dal gruppo 177
- postazioni 188
- proxy 97
- server antivirus 92, 95

espressioni regolari 428, 430

## F

file di configurazione
- Centro gestione 384
- proxy 389
- repository 364
- server antivirus 375

file di stato 372, 373

# Indice analitico

funzioni
agent 103
Dr. Web ESS 16
server antivirus 99

## G

gruppi 169
aggiunzione workstation 177
configurazione 179
configurazione, copiatura 183
eliminazione workstation 177
impostazioni, ereditarietà 180
primari 180
gruppi predefiniti 169
gruppi primari 180

## I

icone
agent 104
lista gerarchica 116
scanner di rete 74, 130
impostazioni DBMS 333
indirizzi di posta 241
indirizzo di rete 357
Enterprise Agent/ Installer 361
Enterprise Server 360
installazione
agent 55, 64
agent, Active Directory 80
agent, su remoto 73, 80
Dr.Web Browser-Plugin 52
NAP Validator 87
server antivirus 34, 46
installazione di rete 400
interfaccia
agent 103, 104
server antivirus 101

## L

licenze 29
licenze per indirizzo, UNIX 241
limitazione di accesso
risorse locali 239
limitazione di aggiornamento 311
lingua
Centro gestione 122, 165
log di server 263

## M

messaggi
formato logotipo 244
invio all'utente 241
modalità mobile di agent 312

## N

NAP Validator 322
configurazione 324
installazione 87
nuova 186, 200

# Indice analitico


## O

office control 239
orario
- aggiornamenti 307
- centralizzato 206
- locale 210
- server 264

## P

pacchetto antivirus
- componenti, composizione 189
- contenuti 19
- eliminazione 92, 189
- installazione 64, 80, 189

parti distribuzione 28
procedure 436
proprietà di workstation 189
protocollo del server 100
proxy
- aggiornamento 303
- avvio, arresto 321
- eliminazione 97
- file di configurazione 389
- funzioni 317
- installazione 88

## Q

quarantena 236

## R

registrazione
- postazioni sul server 186
- prodotto Dr.Web 29

relazioni tra server
- configurazione 276
- tipi 273

repository 268
- aggiornamento 309
- editor repository 270
- parametri generali 269

requisiti di sistema 21, 326
rete antivirus 273
- aggiornamenti 284
- componenti 17, 143
- eventi virus 284
- impostazione legami 276
- licenze 30
- programmazione 32
- struttura 143, 273

ripristino
- DB (database) 530
- server antivirus 537

ripristino workstation 188

## S

SAM
- vedi anche aggiornamento manuale 305

# Indice analitico

scanner
antivirus 211, 419
di rete 73, 128
scanner antivirus 419
scansione
automatica 206
manuale 211
scansione antivirus 211
server antivirus
aggiornamento, per SO UNIX 294
aggiornamento, per SO Windows 287
avvio 101
chiavi di avvio 403
configurazione 247
contenuti di cartella 45
eliminazione, per SO UNIX 95
eliminazione, per SO Windows 92
file di configurazione 375
impostazione legami 276
installazione, per SO UNIX 46
installazione, per SO Windows 34
interfaccia 101
log 263
orario 264
protocollo 100
ripristino 537
task 99
tipi di legami 273
trasporto 520
sincronizzazione, componenti 305
statistiche
workstation 226

## T

traffico
codifica 256
compressione 256
contenuti 146

## U

utenze 163, 164
workstation, creazione 55

## V

variabili di ambiente 422

## W

workstation
aggiunzione al gruppo 177
configurazione 189
configurazione, copiatura 183
configurazione, ereditarietà 180
connessione 186
creazione record 55
eliminazione 188
eliminazione dal gruppo 177
gestione 185
non confermata 186

# Indice analitico

workstation
- nuova 186
- proprietà 189
- ripristino 188
- scansione 206, 211
- statistiche 226

© 2004-2013 Doctor Web